Data Processing Agreement

Rflect AG

Version: 16 June 2026

1. Subject matter of the agreement

1.1 Description. Rflect AG, with its registered office in Zurich, Switzerland, postal address c/o Ivan Jovanovic, Neunbrunnenstrasse 118, 8050 Zürich, registered in the Commercial Register of the Canton of Zurich under company number CHE-402.686.433 (the "**Processor**"), provides a software-as-a-service solution to support educational processes to the customer (the "**Controller**").

1.2 Preamble. This agreement sets out the data-protection framework and the obligations for handling personal data in accordance with Regulation (EU) 2016/679 (GDPR), the Swiss Federal Act on Data Protection (FADP), the cantonal data-protection laws applicable to the Controller where relevant, and other applicable data-protection laws (together, "**Data Protection Law**").

1.3 Relationship. The Controller is the data controller for all personal data of Authorised Users (students, lecturers, teaching assistants, coaches and other natural persons granted access to the Services by the Controller) processed through the Services. The Processor acts exclusively as data processor on behalf of the Controller and processes personal data only on the Controller's documented instructions.

1.4 Scope. The Processor provides services under the Institutional Terms of Service and the Order Form (together, the "**Contracts**"). The scope, purpose and duration of the processing are defined in the Contracts and, where applicable, in supplementary written instructions of the Controller.

1.5 Term. This agreement applies for the term of the Contracts and survives until the Processor has returned or deleted all personal data processed on the Controller's behalf in accordance with Section 11.

1.6 Order of precedence. In the event of conflict between this agreement and the Contracts on matters of personal-data processing, this agreement prevails.

2. Nature, purpose and categories of processing

2.1 Nature and purpose. The Processor processes personal data to operate the Rflect platform, to enable reflective learning activities, to provide insights to lecturers based on shared reflections, and to deliver AI-supported educational features to Authorised Users where they have opted in.

2.2 Categories of data subjects. Authorised Users (students, lecturers, teaching assistants, coaches, administrators) of the Controller.

2.3 Categories of personal data.

- Account data: email address, name, surname and related identifiers.
- Self-assessment data: gender and age range (where collected for academic-study purposes).
- Institutional affiliation: programme, class, cohort and related context.
- Reflection content submitted by Authorised Users. The Processor recognises that reflection content may contain data on the intimate sphere, on health or otherwise particularly sensitive personal data within the meaning of Art. 5 lit. c FADP / Art. 9 GDPR, and that AI-supported analysis of reflection content may amount to profiling under Art. 5 lit. g FADP / Art. 22 GDPR.
- Usage logs and technical metadata generated by use of the Services.

2.4 Sharing model. Authorised Users set a sharing status for each reflection: private, shared with lecturer, shared with class, or shared with class anonymously. The Processor implements this sharing status as both a technical and a legal access boundary, as further set out in Section 2.5.

2.5 Private reflections - standing instruction and carve-out. The Controller acknowledges that reflections marked "private" by Authorised Users are, by design and by contract, not accessible to the Controller, its lecturers, its coaches or its administrators. The following standing arrangements apply, irrevocably, for the term of this agreement and beyond:

(a) The Controller waives, in advance, any right to (i) access reflections marked "private", (ii) instruct the Processor to disclose them or to surface them in dashboards, lecturer or coach views, exports or reports, or (iii) require aggregate statistics that would allow re-identification of private content.

(b) This standing instruction may not be amended, suspended or overridden by side letter, change order, oral arrangement or any amendment of this agreement, except by a written amendment that simultaneously and transparently re-consents the affected Authorised Users with prior in-app notice.

(c) On termination of the Contracts, private reflections are deleted or, at the option of the Authorised User, returned to that user and never to the Controller.

(d) This Section 2.5 is concluded as a genuine third-party stipulation in favour of Authorised Users within the meaning of Art. 112(2) OR: Authorised Users may invoke the Controller's waiver directly.

(e) If the Processor receives a binding court order, regulatory demand or criminal-procedure request that requires it to surface private content, the Processor will notify the Controller (and, where permitted, the affected Authorised User) without undue delay and will, to the extent legally permissible, delete the affected private reflections rather than release them.

(f) Audits permitted under Section 8 may verify the technical separation between private and shared reflection content, but may not be used to access private content.

(g) The Processor does not review private reflection content through its own personnel and does not surface private reflection content on Processor-internal dashboards. This commitment is subject only to Section 2.5(e) (binding court order, regulatory demand or criminal-procedure request).

The Processor warrants in the technical and organisational measures (Annex 3) that private reflections are architecturally inaccessible to Controller-side dashboards and administrative roles.

2.6 AI-supported features. The Processor distinguishes between AI processing of shared reflections and AI processing of private reflections:

(a) **Shared reflections.** AI-supported features that operate on reflections shared with a lecturer, with a class, or with a class anonymously (for example, AI-supported insights and assistance for lecturers, such as the "Teaching Assistant" feature) are provided under this agreement on the Controller's general instruction. No separate Authorised User opt-in is required, because the user has already chosen to share the reflection.

(b) **Private reflections.** AI processing of reflections marked "private" (for example, the "Go Deeper" feature, providing personalised feedback to the Authorised User on their own reflection) is provided only where the Authorised User has given a separate, granular in-app opt-in. The Controller has no role in obtaining or withdrawing this opt-in; it is collected and managed by the Processor on a user-by-user basis in accordance with Art. 6(7) FADP / Art. 9(2)(a) GDPR. The Controller acknowledges that it cannot consent on behalf of an Authorised User to AI processing of private reflections, in particular where the content is particularly sensitive personal data. Withdrawal of the opt-in takes effect immediately for all future AI processing of that user's private reflections.

(c) **No model training.** Reflection content as well as lecturer created content is not used to train AI models, whether by the Processor or by sub-processors.

(d) **AI inference processing.** AI inference for AI-supported features runs through EU inference endpoints operated by the AI inference sub-processor identified in Annex 2. To reduce latency and cost, the request prompt may be held in the sub-processor's ephemeral, encrypted prompt cache for up to one (1) hour from last use, after which it is automatically deleted. The cache stays within the EU inference environment, is not accessible to the Processor's personnel, and is never used to train AI models (Section 2.6(c)). No input or output is otherwise retained beyond the inference request.

3. Processor's obligations

3.1 Documented instructions. The Processor processes personal data only on the Controller's documented instructions, including with regard to transfers to a third country. The Contracts and this agreement constitute the initial instructions. The Controller may amend or supplement instructions in writing or text form at any time. Where the Processor is required by Swiss or EU law to process data otherwise, it will inform the Controller of that legal requirement before processing, unless the law prohibits such notice.

3.2 Confidentiality. The Processor ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and have been instructed in the relevant data-protection requirements before processing.

3.3 Use of personal data by the Processor.

(a) The Processor does not process personal data for its own purposes outside the operation and improvement of the Services.

(b) For the operation and improvement of the Services, the Processor may review shared reflection content (reflections that an Authorised User has chosen to share with their lecturer, with their class, or anonymously with their class) and outputs generated by Rflect features on the basis of such shared content (for example, conversations with the Teaching Assistant), in order to investigate user-reported issues, evaluate response quality, detect failure modes, and iterate on the prompts, guardrails and configuration of the Services. This is distinct from the training of AI models (which is excluded under Section 2.6(c)) and does not extend to reflection content marked private. Such review is carried out by personnel subject to the confidentiality undertaking in Section 3.2.

(c) The Processor may also use anonymised data for performance reporting and academic publications. Anonymisation must be irreversible and verified before such use.

3.4 Data-subject rights assistance. The Processor assists the Controller, taking into account the nature of the processing and the information available to the Processor, in fulfilling its obligations under Arts. 12–22 GDPR / Arts. 25–32 FADP, including responding to requests for access, rectification, erasure, restriction, portability and objection. If an Authorised User exercises rights by contacting the Processor directly, the Processor informs the Controller without undue delay and awaits the Controller's instructions before taking action, except where the Processor is required by Data Protection Law to act on the request itself.

3.5 Compliance assistance. The Processor assists the Controller in complying with its obligations under Arts. 32–36 GDPR / Arts. 7–24 FADP, including security measures, breach notification, data protection impact assessments and prior consultation, taking into account the nature of the processing and the information available to the Processor.

3.6 Data portability and account migration.

(a) **Standing authorisation.** The Controller authorises the Processor, as a standing instruction granted once under this agreement, to let any Authorised User export or migrate the personal data that the user has themselves authored, on that user's own request and without further approval from the Controller.

(b) **Scope.** This covers reflections and other content authored by the Authorised User - irrespective of sharing setting (private, shared with lecturer, or shared with class) - together with feedback directed specifically to that user. It does not extend to content authored by or about other data subjects, including other students' reflections, class or group threads, and cohort-level data.

(c) **Copy, not removal.** Export or migration is provided as a copy or transmission to a destination of the user's choice. It does not delete or alter the Controller's own records, which the Controller retains.

(d) **Migration window.** Where the Controller removes or de-provisions an Authorised User's account, the Processor holds deletion of that user's authored data for thirty (30) days, during which the user may exercise the right in (a). After that window, the Processor completes deletion in accordance with Section 11.

4. Technical and organisational measures

4.1 The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Art. 32 GDPR / Art. 8 FADP. The measures in force at the date of this agreement are set out in Annex 3 (Technical and Organisational Measures).

4.2 Backup and retention. The Processor maintains a tiered backup regime (daily incremental, daily, weekly and monthly snapshots). Backup retention periods are specified in Annex 3. The Processor operates a documented restore process under which deletion requests received between the snapshot date and any restore date are re-applied automatically, so that data deleted at the request of the Controller or an Authorised User is not re-introduced into the production system by a restore.

4.3 Material changes. The Processor reviews the technical and organisational measures regularly and notifies the Controller of material changes that affect the security of the processing.

5. Sub-processors

5.1 General authorisation. The Controller authorises the engagement of the sub-processors listed in Annex 2. The Processor maintains the up-to-date list of sub-processors and the description of their processing.

5.2 Change notice and objection. The Processor notifies the Controller in writing at least within **30 days** upon engaging a new sub-processor or replacing an existing one. The Controller may object to the change on reasonable data-protection grounds within that 30-day period. If the Processor cannot accommodate the objection, the Controller may terminate the Contracts in respect of the affected Services on reasonable notice, without penalty.

5.3 Equivalent obligations. The Processor binds each sub-processor by written contract to data-protection obligations substantially equivalent to those set out in this agreement, in particular with regard to confidentiality, security measures, sub-processing, international transfers and assistance with data-subject rights.

5.4 International transfers. Where a sub-processor processes personal data outside Switzerland and the EEA, the Processor implements an appropriate transfer mechanism (EU

Standard Contractual Clauses with the Swiss addendum issued by the FDPIC, reliance on the Swiss-US Data Privacy Framework where applicable, or another mechanism recognised under Data Protection Law) and conducts a transfer-impact assessment that it makes available to the Controller on request.

6. Breach notification

6.1 Notification. The Processor notifies the Controller of any confirmed or suspected personal-data breach without undue delay and in any event within **24 hours** of becoming aware of it, providing at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and records concerned;
- the name and contact details of the Processor's data-protection contact;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to address the breach and to mitigate its possible adverse effects.

6.2 Mitigation. The Processor takes all reasonable measures without undue delay to contain the breach and to mitigate its consequences for data subjects and for the Controller.

6.3 Third-party events. If the Controller's data at the Processor are jeopardised by attachment, seizure, insolvency proceedings or any other third-party measures, the Processor informs the Controller without undue delay, unless prohibited by court order or law. The Processor informs the relevant authorities and counterparties that decision-making authority over the data lies exclusively with the Controller.

7. Right to issue instructions

7.1 The Processor processes personal data only within the scope of the Contracts and on the Controller's instructions, subject to Section 3.1.

7.2 Authorised persons. Instructions may be given by the persons identified in Annex 1 (Authorised Persons). For the Controller, all active lecturer accounts and the contact identified by the Controller as its data-protection contact are authorised to issue instructions in relation to data they administer.

7.3 Unlawful instructions. If the Processor considers that an instruction infringes Data Protection Law, it notifies the Controller without undue delay. The Processor may suspend the execution of the instruction until the Controller has confirmed or modified it, and may decline to execute a manifestly unlawful instruction.

8. Audit rights

8.1 The Controller is entitled to verify the Processor's compliance with this agreement and with Data Protection Law within an appropriate scope. The Controller exercises its audit

rights only to the extent required to meet its legal obligations and in a manner that does not unduly disrupt the Processor's operations.

8.2 The Processor provides the Controller, within a reasonable deadline, with the information and documentation required to evidence compliance, including independent audit reports (such as ISO 27001) where available. On-site audits may be carried out on reasonable notice.

8.3 Audit rights are subject to the limitations in Section 2.5(f) regarding private reflections.

9. Liability

Liability is governed by the applicable Data Protection Law and, where the Contracts contain a more specific provision, by the Contracts. Liability for intent, gross negligence, personal injury and fraud is not excluded (Art. 100(1) OR; Art. 199 OR).

10. Extraordinary right of termination

The Controller may terminate the Contracts without notice in full or in part if the Processor materially breaches this agreement, intentionally or with gross negligence violates Data Protection Law, or is unable or unwilling to execute a lawful instruction of the Controller. For minor (non-intentional, non-grossly negligent) breaches, the Controller grants the Processor a reasonable cure period.

11. Termination

11.1 Return or deletion. On termination of the Contracts and at the option of the Controller, the Processor returns or deletes all personal data processed on the Controller's behalf, and deletes existing copies, unless retention is required by Swiss or EU law. The Processor maintains documentation of the deletion and provides a certificate of deletion on request.

11.2 Exception for private reflections. Section 2.5(c) applies to private reflections: these are deleted or returned to the Authorised User at the user's option and then deleted, never to the Controller.

11.3 Surviving confidentiality. The confidentiality obligations in Section 3.2 survive termination.

12. Concluding terms

12.1 No retention beyond term. The Processor has no right to retain personal data under this agreement beyond the Contracts' duration unless required by law.

12.2 Form. Amendments and supplements to this agreement, including any change to this form requirement, must be in writing.

12.3 Relationship to Contracts. The Contracts remain in force unless inconsistent with this agreement, in which case this agreement prevails on matters of personal-data processing.

12.4 Severability. If any part of this agreement is or becomes invalid, the remaining parts remain in force. The parties replace the invalid term with one that best reflects the original economic purpose.

12.5 Governing law. Swiss substantive law, together with the material Union law applicable to the processing, including the GDPR.

12.6 Jurisdiction. Exclusive jurisdiction lies with the competent court of Zurich, Switzerland.

Annex 1 — Authorised persons

On the part of the Processor (by function, not by name):

- Data-Protection Contact, reachable at `privacy@rflect.ch`.
- Customer Support, reachable at `support@rflect.ch`.

On the part of the Controller:

- All active lecturer accounts of the Controller.
- The data-protection contact identified by the Controller in the Order Form.

Annex 2 — Approved sub-processors

Name	Description of processing	Location of processing	Third-country transfer
AWS	Infrastructure-as-a-service: hosting of the application, the database, logs, backups and all in-transit data through AWS cloud services. Additionally, the Processor uses **AWS Bedrock** AI inference to deliver AI-supported features. Where students opt in, private reflection content (which may include name and email address) may be processed through AWS Bedrock to generate personalised feedback and insights. Students cannot opt out of processing of shared reflections by AWS Bedrock. All AI inference processing occurs within the EU. To reduce latency and cost, AWS Bedrock may hold the request prompt in an ephemeral, encrypted prompt cache within the EU inference environment for up to one (1) hour from	EU	None

	last use, after which it is automatically deleted; AWS Bedrock does not otherwise store data beyond the inference request and does not use customer data for model training.		
Friendly Analytics	General application-use analytics	Switzerland	None
Sentry	Application logs, error analytics and user-behaviour analytics in error situations	EU / Frankfurt	None
Pipedrive (CRM)	CRM and onboarding workflows. Receives account and event data (name, email, programme, signup and invitation events) relating to lecturers and student invitations, transmitted via webhook.	EU / Frankfurt	None

Sub-processor data-protection terms:

- AWS — Data Processing Addendum: https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf
- Friendly Analytics — Data Processing Agreement: https://friendly.ch/en/privacy/dpa
- Sentry — Data Processing Addendum: https://sentry.io/legal/dpa/
- Pipedrive — Data Processing Addendum: https://www.pipedrive.com/en/privacy/dpa

Annex 3 — Technical and organisational measures (summary)

- **Architectural separation of private reflections.** Private reflection content is stored and access-controlled such that it is not retrievable through Controller-side or Processor-internal dashboards, administrative roles or reporting endpoints, and is not surfaced in AI workflows other than the user's opted-in features.
- **Access control.** Access to production systems and internal administration tools is restricted to authorised Processor personnel bound by confidentiality (Section 3.2).
- **Encryption.** Encryption in transit (TLS) and at rest (AWS-managed keys) for production data; encryption of backups.
- **Logging and monitoring.** Centralised logging, application error monitoring, security alerting.
- **Backups.** Daily incremental and full database backups, with weekly and monthly snapshots. Retention as defined in the operational backup policy. A documented restore process re-applies deletions received between the snapshot date and the restore date.
- **Sub-processor security.** Contractual confidentiality, data-protection and security commitments from each sub-processor as set out in Section 5.
- **Incident response.** Documented incident-response procedures, including breach notification within the timeframes in Section 6.