DATA PROCESSING ADDENDUM ("DPA")

STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS

(October 20, 2026)

For the purposes of Standard Contractual Clauses Module 2 ("SCC Module 2") and the UK Addendum, Customer is the data exporter and CoLab AI Inc. ("CoLab") is the data importer. If and to the extent an Affiliate of either CoLab or Customer relies on SCC Module 2 or the UK Addendum for the transfer of Personal Data, any references to "Customer" in this Schedule, shall include such Affiliate. This DPA incorporates the official English-language text of Module 2 of the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council) found at: http://data.europa.eu/eli/dec_impl/2021/914 and the UK Addendum found at: found at https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf.

The Parties agree to the following:

1. **Instructions.** This Data Processing Addendum ("DPA") and the Subscription Agreement are Customer's complete and final documented instructions to CoLab at the time of the later of the signature to the applicable Order Form for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Subscription Agreement.

For the purposes of clause 8.1(a) of SCC Module 2, the instructions by Customer to Process Personal Data are as follows: Processing in accordance with the Subscription Agreement and applicable Order Form(s) and shall include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

2. **Docking clause.** The option under clause 7 shall not apply.

3. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of SCC Module 2 shall be provided by CoLab to Customer only upon Customer's written request.

4. **Security of Processing.** For the purposes of clause 8.6(a) of SCC Module 2, Customer is responsible for making an independent determination as to whether the technical and organizational measures set forth in Annex II (found in Schedule 1 of this DPA) meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by CoLab provide a level of security appropriate to the risk with respect to its Personal Data.

5. **Audits of the SCCs.** The parties agree that the audits described in clause 8.9 of SCC Module 2 shall be carried out as follows:

5.1. **Audit Program**. CoLab shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA, including those obligations required by applicable Data Protection Laws and Regulations, as set forth in this section 5.

5.2 **Access to Third-Party Certifications and Audits Information.** Upon Customer's written request, but no more than once per year, and subject to the confidentiality obligations set forth in the Agreement, CoLab shall:

(i) make available to Customer information regarding CoLab's compliance with the obligations set forth in this DPA in the form of a copy of CoLab's most recent third-party certifications;

(ii) upon request, provide Customer with certificates of third-party auditors' audits of Sub-processors that have been provided by those Sub-processors to CoLab or inform Customer where they might independently access such publicly-available certificates.

5.3 **On-Site Audit.** Customer can request an on-site audit of CoLab's Processing activities covered by this DPA ("On-Site Audit") only when: (i) the information available pursuant to section "Access to Third-Party Certifications and Audits Information" is not sufficient to demonstrate compliance with the obligations set out in this DPA; or (ii) Customer has received a notice from CoLab of a Security Breach affecting Personal Data. Any On-Site Audits will be limited to Customer Data Processing facilities operated by, and under the control of, CoLab. An On-Site Audit may be conducted by Customer either itself or through a Third-Party Auditor (as defined below in section 5.6) selected by Customer.

5.4 **Reasonable Exercise of Rights.** An On-Site Audit shall be conducted by Customer or its Third-Party Auditor: (i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Customer; (ii) up to one time per year with at least eight weeks' advance written notice. If an emergency justifies a shorter notice period, CoLab will use good faith efforts to accommodate the On-Site Audit request; and (iii) during CoLab's normal business hours, under reasonable duration and shall not unreasonably interfere with CoLab's day-to-day operations.

5.5 **Scope, Timing Duration of Audit**. Customer acknowledges that CoLab operates a multi-tenant cloud environment. Before any On-Site Audit commences, Customer and Colab shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of CoLab. CoLab shall have the right to reasonably adapt the scope of any On-Site Audit to negate risks with respect to, and including, service levels, availability, and confidentiality of other CoLab customers' information.

5.6 **Third-Party Auditor**. A Third-Party Auditor means a third-party independent contractor. An On-Site Audit can be conducted through a Third Party Auditor if: (i) prior to the On-Site Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect CoLab's proprietary information and the confidential information of third parties; and (ii) the costs of the Third-Party Auditor are at Customer's expense.

5.7 **Findings**. Customer must promptly provide CoLab with information regarding any non-compliance discovered during the course of an On-Site Audit.

6. **General Authorization for Use of Sub-processors**. For the purposes of clause 9(a) of SCC Module 2, CoLab has Customer's general authorization (Option 2) to engage Sub-processors in accordance with this Section 6.

6.1 Customer acknowledges and agrees that CoLab may engage third-party Sub-processors to provide support to the Services. The current list of Sub-processors engaged in Processing Personal Data, including a description of their processing activities and countries of location, is listed in Annex III. Customer hereby consents to CoLab's use of these Sub-processors, their locations and processing activities as it pertains to Personal Data.

6.2 CoLab has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

7. **Notification of New Sub-processors and Objection Right for New Sub-processo**rs. Pursuant to clause 9(a) of SCC Module 2, Customer acknowledges and expressly agrees that CoLab may engage new

Sub-processors as described in this Section 7. CoLab shall inform Customer of any changes to Sub-processors following the procedure provided for in Section 7 of this DPA.

7.1 **New Sub-processors**. CoLab shall provide notification of a new Sub-processor(s) at least thirty (30) days before authorizing any new Sub-processor(s) to Process Personal Data. Customer may object to CoLab's use of a new Sub-processor by notifying CoLab promptly in writing at privacy@colabsoftware within fourteen (14) days of receipt of CoLab's notice. CoLab and Customer may engage in discussions in good faith as to the suitability of a new Sub-processor. If Customer continues to object to the use of a new Sub-processor, Customer may terminate the Agreement by providing written notice to CoLab within thirty (30) days of receipt of CoLab's notice. CoLab will refund Customer any prepaid fees covering the remainder of the Subscription Term of any Order Form(s) following the effective date of termination.

8. **Liability**. CoLab shall be liable for the acts and omissions of its Sub-processors to the same extent CoLab would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

9. **Complaints**. For the purposes of clause 11 of SCC Module 2, CoLab shall inform Customer if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. CoLab shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

10. **Precedence**. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11. Annex I-A to SCC Module 2 shall be completed as follows:

LIST OF PARTIES

Data exporter(s): Customer name as noted on the applicable Order Form

Activities relevant to the data transferred under these Clauses:

Access to CoLab Services pursuant to a Services Agreement signed between the parties

Role (controller/processor): Controller

Data importer(s):

Name: CoLab AI Inc.

Address: 5 Springdale Road, St. John's, Newfoundland and Labrador, Canada A1E 0E4

Contact person's name, position and contact details:

Adam Keating, CEO, adam@colabosftware.com

Robert Percy, VP Security, robertpercy@colabsoftware.com

Colette Goodyear, General Counsel, colettegoodyear@colabsoftware.com

privacy@colabsoftware.com

Activities relevant to the data transferred under these Clauses:

Provision of CoLab Services pursuant to a Services Agreement signed between the parties.

Role (controller/processor): Processor

12. Annex I-B to SCC Module 2 shall be completed per Schedule A to this Exhibit.

13. Annex I-C to SCC Module 2 shall be completed as follows:

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority is Irish DPC.

CoLab Software has appointed Lewis Silkin as its EU Representative.

Contact : EUrep.CoLabSoftware@lewissilkin.com

14. Annex I-D to SCC Module 2 shall be completed as follows:

SERVICES AGREEMENT

In these Clauses, Services Agreement means the agreement between the data exporter and the data importer entitled Subscription Agreement.

15. Annex II to SCC Module 2 shall be completed per Schedule B to this Exhibit.

16. Annex III to SCC Module 2 shall be completed per Schedule C to this Exhibit.

17. The UK addendum shall be completed per Schedule D to this Exhibit.

18. Signature of the applicable Order Form shall be deemed to constitute signature and acceptance of the DPA and the Standard Contractual Clauses.

SCHEDULE A

ANNEX I - B

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of the CoLab Services to whom Controller has assigned logins, primarily employees

The categories of personal data transferred are:

First Name, Last Name, Work email addresses

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not Applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Individual email addresses will be transferred only once to supplier to gain the access to the tool and then used to log in to the tool.

In general, data is transferred continuously as Controller activates/deactivates, assigns/reassigns login credentials.

Nature of the processing

Log into and utilization of the Services pursuant to the Services Agreement between the parties.

Purpose(s) of the data transfer and further processing

CoLab will process Personal Data as necessary in order to provide the Services pursuant to the Services Agreement between the parties.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As long as user email address is active. CoLab retains PII in its audit logs containing access information indefinitely for security purposes.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

PII is transferred to Sub-processors for the purpose of providing the Services as described in the Services Agreement

SCHEDULE B

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The data importer will implement the measures set out or provided for in the Services Agreement. This includes:

1 Measures of pseudonymisation and encryption of personal data;

PII is limited within the application. This data is anonymized as per GDPR requirements.

The CoLab system utilizes full end-to-end encryption with all data encrypted using industry standard encryption mechanisms. All data in transit is encrypted utilizing Transport Layer Security (TLS) 1.2 or greater via AWS.

Customer data is encrypted at rest using AES 256 encryption with separate encryption keys per customer.

2 Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;

CoLab is built to the highest standards of security and data protection, adopting a security-first approach to product development and infrastructure design: https://www.colabsoftware.com/security. CoLab utilizes a WAF, AWS Network Firewall and AWS Security Groups. CoLab has implemented an architecture with no requirement for web or application servers to have public IP addresses.

In our AWS environment, AWS GuardDuty uses VPC flow logs, Cloudtrail audit logs, and other data to provide IDS capabilities. All logs generated by these technologies are sent to our log management solution where alerts are configured for both known cybersecurity attacks and for anomalies specific to the CoLab application. The alerts are sent to CoLab's security and operations team in real-time via Slack, email, and if high severity, via call.

CoLab follows a least privilege model. Permissions are assigned based on job function for both privileged and non-privileged accounts. Quarterly access reviews are completed for all user accounts to ensure the ongoing relevance of access.

All endpoints have Microsoft Defender ATP installed with automatic updates.

Weekly vulnerability scans are performed on production and corporate environments. Bi-weekly reviews are performed by the Security team and remediation tasks are assigned to respective support teams.

CoLab follows industry standard incident response procedures and both federal and regional breach notification requirements. The communication timeline for notifying impacted customers is within 24 hours following confirmation of Security Breach.

CoLab’s password policy is configured inline with NIST Special Publication 800-63B. This includes a requirement for the password to be at least 10 characters in length and not match a list of common or known compromised passwords. Users are prevented from further authentication attempts following 10 failed logins. All failed login attempts are logged and monitored with alerting for anomalous login behaviours. Customer password policies can be enforced through SSO integration to their identity provider.

Privileged access is managed through an access request process. CoLab employees do not have permission to access customer data unless explicitly granted written permission by the customer for support purposes only.

Customer data is encrypted at rest using AES 256 encryption with separate encryption keys per customer.

Background checks are done for all CoLab personnel regardless of job role. Formal background checks are completed by an external vendor for employment experience, education and criminal history.

Customer uploaded data files use folder level separation in AWS S3 with the necessary authentication, authorization and access controls implemented to ensure that users of the CoLab service can only access their company data and the data they have been authorized to access.

Additional details pertaining to CoLab’s security program and controls can be found in CoLab’s SOC 2 reports and ISO audits.

3 Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

Customer data housed in the file storage service is synchronously stored across multiple AWS data centers in Canada. Database backups are replicated to multiple AWS data centers with continuous and full snapshots taken every 12 hours and retained as per CoLab's Information Management policy.

CoLab’s Business Continuity and Disaster Recovery Plans (DRP) define backup restoration and recovery procedures. Management reviews, tests, and approves the plans annually for ongoing relevance and to confirm the reliability and integrity of system backups and recovery operations.

4 Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing;

The security team is involved early in the lifecycle, working with product, design and development teams to assist with security requirements and threat modeling. A security team member is assigned to build teams throughout a build cycle to identify risks, provide feedback and perform security testing.

Penetration testing and security assessments are conducted regularly by CoLab’s Security Team. Third party penetration tests are conducted annually.

5 Measures for user identification and authorisation;

Privileged access to the production environment is via a TLS encrypted tunnel that can only be established with a CoLab user account, from a compliant CoLab device, using multi-factor authentication and appropriate role assignments.

Privileged access is managed through an access request process and roles are assigned based on job function. Privileged access is granted only to employees with a legitimate business need and relevant job role. Roles and their corresponding permissions are also reviewed quarterly to maintain the principle of least privilege.

Each employee has one unique Azure AD account except for Administrators who have a separate administrator account for performing elevated functions. The creation of service accounts not associated with a named user, generates an alert within the SIEM tool for investigation and remediation by the Security team.

6 Measures for the protection of data during transmission;

All data in transit is encrypted utilizing Transport Layer Security (TLS) 1.2 or greater via AWS.

7 Measures for the protection of data during storage;

Customer data is encrypted at rest using AES 256 encryption with separate encryption keys per customer.

8 Measures for ensuring physical security of locations at which personal data are processed;

Physical security for AWS data centers is managed by AWS. Please refer to AWS data center security controls documentation: https://aws.amazon.com/compliance/data-center/.

9 Measures for ensuring events logging;

All security relevant logs and events are sent to our log management system on write. Critical audit logs are retained indefinitely; non-critical logs are retained for a minimum of one year. Customer specific logs can be exported from within the application for a 90 period.

10 Measures for ensuring system configuration, including default configuration;

CoLab has documented standards and processes for infrastructure and software hardening and configuration. Containers and servers are deployed using standard images and assessed against CIS benchmarks using an automated vulnerability management service.

CoLab infrastructure is built using official Ubuntu server based prebuilt images. Ubuntu servers are configured to install security updates nightly and are rebuilt at least once a month as part of the release process.

11 Measures for internal IT and IT security governance and management;

CoLab’s leadership directs the creation, implementation, and enforcement of CoLab’s policies and procedures to communicate expectations and effectively safeguard internal and external data. Policies and

procedures are reviewed annually, as well as in response to changes in business requirements, and updated as required.

CoLab has a risk management process in place for identifying, assessing, and managing risks. The Security Steering Committee, comprised of executive and leadership from each of the functional areas, review identified risks, mitigations and control improvements on a quarterly basis. Risks and associated mitigations are tracked and monitored via the risk register. The Vice President of Security and the Director of Risk and Compliance are responsible for evaluating and tracking risks.

12 Measures for certification/assurance of processes and products;

CoLab completes a SOC 2 Type II annually. CoLab also has achieved ISO 27001, ISO 27017, ISO 27018, and TISAX AL3 certifications.

13 Measures for ensuring data minimisation;

Colab collects the minimum PII necessary – full name and email address - in order to provide the CoLab Services and does not collect any other personally identifiable information from our Customers. Only customer administrative users are able to access this information for their users within the application.

14 Measures for ensuring data quality;

File storage for uploaded files has versioning enabled for object modifications and provides an integrity check in responses. Regular integrity checks are performed on objects using checksums and if corruption is detected it is repaired using redundant data. There is also calculation of checksums for all network traffic as part of the file upload or download to detect corruption.

15 Measures for ensuring limited data retention;

CoLab retains only the data that is necessary to effectively conduct its business activities, provide services to Customers and comply with applicable laws and regulations. CoLab has defined data retention and deletion periods and will ensure that deletion of Customer Data is conducted in a manner that safeguards the security and confidentiality of the information.

16 Measures for ensuring accountability;

Customer data is protected at all times. Any vendors (subprocessors) are vetted through a vendor management process which includes an assessment of the vendors security arrangements and commitment to privacy. Legal contracts with vendors include appropriate data privacy provisions, clauses and remedies.

CoLab employees sign non-disclosure agreements as a condition of their employment and receive training in their obligations respecting privacy and confidentiality of customer data.

Internal personnel at CoLab regularly review and make updates to security practices to ensure they support the functioning of internal controls. These controls include the continuous monitoring and remediation of potential threats and vulnerabilities in system components. Members of this team are trained and supported to properly evaluate these systems and controls.

Weekly Security meetings are scheduled to review the organization's security posture and any required changes or control improvements.

17 Measures for allowing data portability and ensuring erasure.

Upon expiration of the service agreement, CoLab shall completely destroy all copies of Customer data no sooner than 30 days following the service agreement termination date. At Customers request, CoLab shall have its officers certify in writing that it has destroyed or erased all copies of Customer data in CoLab's possession. The Customer may, within 30 days of the termination or expiration of the agreement, make a request for return of its data. The Customer also has the ability to download its data prior to the termination or expiration of the agreement.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

The data importer will take such measures as are necessary for the data importer to provide such assistance as is necessary to comply with its obligations of assistance under the Clauses.

SCHEDULE C

ANNEX III

LIST OF SUB-PROCESSORS
September 1, 2026

Subprocessor	PII Stored or Processed	Purpose	Location
Amazon Web Services	User name, email, company name, application usage data	Database and application hosting Security and application monitoring Large Language Model (LLM) Provider (used with AI Features only)	Canada and US
Amazon Web Services SES	User name, email, company name, business communications to user	E-mail communication	Canada
Cloudflare WAF	User name, email, company name, application usage data	Application security and monitoring	US
Salesforce	User name, email, company name, business communications	Customer relationship management	US
Datadog	User name, email, company name, application usage data	Log management and monitoring (used with both DES and AI Features)	US
Auth0 by Okta	User name, email, company name, application usage data	User directory and enterprise single-sign on support	US
LaunchDarkly	User name, email, company identifier, application configuration data	Feature Flagging Software	US
Pendo	User name, email, company name, application usage data	Product Experience Platform	US
Hubspot	User name, email, company name	Customer Relationship Management	US
Intercom	Email, company name	Customer Service Platform	US
Mixpanel	User name, email	Product Analytics Platform	US
Retool	User name, email, company name	Software Development Platform	US
Paragon	User name, email, notification consent	Integration Platform as a Services	US
OpenAI	User name, email, company name, application usage data	Large Language Model (LLM) Provider (used with AI Features only)	US

Microsoft Azure	User name, email, company name, application usage data	Large Language Model (LLM) Provider (used with AI Features only, not available in FedRAMP-authorized environment)	Canada and US
Google Cloud	User name, email, company name, application usage data	Large Language Model (LLM) Provider (used with AI Features only)	Global
Turbopuffer	User name, email, company name, application usage data	Large Language Model (LLM) Provider (used with AI Features only, used only in Canada-hosted environment)	Canada
Anthropic	User name, email, company name, application usage data	Large Language Model (LLM) Provider (used with AI Features only, not available in FedRAMP-authorized environment)	Global
WorkOS	User name, email, company name, application usage data	Large Language Model (LLM) Provider (used with AI Features only, not available in FedRAMP-authorized environment)	US

SCHEDULE D
UK ADDENDUM

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	As set out in Annex I of this DPA	As set out in Annex I of this DPA
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Robert Percy Job Title: Chief Information Officer Contact details including email: privacy@colabsoftware.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	Controller to Processor	No	No	General	30 Days	No
3						
4						

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set out in Annex I of the DPA
Annex 1B: Description of Transfer: As set out in Annex I of the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II of the DPA
Annex III: List of Sub processors (Module 2): As set out in Annex III of the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party