

DATA PROCESSING AGREEMENT

Lou Squared Systems Inc. operating as OfficeEaze

Version 1.3

Updated: August 2026 — Corrected to reflect accurate Lovable platform relationship

Effective Date: _____ (to be completed upon execution)

Governed by the laws of the Province of Ontario, Canada

Between

Lou Squared Systems Inc. operating as OfficeEaze

158 Day Road, Castleton, Ontario — privacy@officeeaze.ca

("Processor" / "OfficeEaze")

and

[CUSTOMER LEGAL NAME]

[Customer Province], Canada

("Controller" / "Customer")

What Changed in Version 1.3

Version 1.3 adds Section 3.7 — Dedicated Tenant Environments. This section was added to support Enterprise customers (including dealer groups and franchise networks) who require physical data isolation in addition to the logical row-level security isolation that applies to all OfficeEaze accounts.

Changes from Version 1.2:

1. Section 3.7 (new) — Dedicated Tenant Environments. Sets out the additional obligations that apply where a Customer's account has been designated as a Dedicated Tenant Environment, including: physical isolation of Personal Data in a dedicated AWS ca-central-1 database instance; dedicated API keys and storage credentials; breach scope limitation; data export and secure deletion on termination; and clarification that standard accounts continue to be protected by row-level security under Section 3.2(c).
2. Version references updated throughout from v1.1/v1.2 to v1.3. No other substantive changes. All provisions of Version 1.2 remain in effect.

Recitals

WHEREAS Lou Squared Systems Inc. operating as OfficeEaze provides a cloud-based back-office software platform for Canadian small businesses, including payroll processing tools, HR management, employee onboarding, document generation, and related services (the "Service");

WHEREAS the Customer operates a business in Canada and uses the Service to manage employment records, process payroll, and store personal information about the Customer's employees, contractors, and related individuals (collectively, "Data Subjects");

WHEREAS in providing the Service, OfficeEaze processes personal information on behalf of the Customer as a data processor under applicable Canadian privacy legislation;

WHEREAS the Customer is the data controller and is responsible for determining the purposes and means of processing personal information about its employees and other Data Subjects;

WHEREAS OfficeEaze currently operates on Lovable's Pro plan and, per Lovable's published Data Processing Agreement terms, DPA coverage is included automatically for customers on Lovable's Business or Enterprise plan tier; OfficeEaze commits to upgrading to a Business-tier Lovable plan no later than its first paying customer, at which point Lovable's DPA will apply under Lovable's standard terms; as of today OfficeEaze has no paying customers and has not itself separately executed a DPA with Lovable, and in the interim relies on Lovable's SOC 2 Type II and ISO 27001:2022 certifications and its published subprocessor list;

WHEREAS both parties wish to establish the terms under which processing of personal information occurs, in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA), applicable provincial privacy legislation, and any future Canadian federal privacy legislation that may replace or amend PIPEDA;

NOW THEREFORE, in consideration of the mutual covenants herein and the service relationship established under the Terms of Service, the parties agree as follows:

Section 1 — Definitions

In this Agreement, the following terms have the meanings set out below:

1.1. "Agreement"

means this Data Processing Agreement, including all Schedules attached hereto, as amended from time to time in accordance with Section 18.

1.2. "Applicable Privacy Law"

means the Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, the Freedom of Information and Protection of Privacy Act (Ontario), the Personal Health Information Protection Act (Ontario) where applicable, and any successor or replacement legislation, together with all regulations, guidance notes, and binding decisions issued thereunder. Where the Customer operates in a province with its own substantially similar privacy legislation (Alberta, British Columbia, or Quebec), the applicable provincial law also forms part of Applicable Privacy Law.

1.3. "Controller"

means the Customer — the party that determines the purposes and means of processing Personal Data.

1.4. "Data Breach"

means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Data transmitted, stored, or otherwise processed by OfficeEaze.

1.5. "Data Subject"

means an identified or identifiable natural person to whom Personal Data relates, including employees, former employees, contractors, and job applicants of the Customer whose information is stored in the Service.

1.6. "Personal Data"

means any information about an identifiable individual that is processed by OfficeEaze on behalf of the Customer in connection with the Service, including but not limited to: full legal name, home address, date of birth, Social Insurance Number (SIN), employment income, banking and direct deposit details, T4 and tax slip data, work schedule and hours, employment agreements, performance records, medical information entered into the Service, and any other information as further described in Schedule A.

1.7. "Platform DPA"

means Lovable Inc.'s published Data Processing Agreement, which under Lovable's own terms is incorporated automatically for customers on Lovable's Business or Enterprise plan tier. OfficeEaze currently operates on Lovable's Pro plan and has not itself separately executed a DPA with Lovable; OfficeEaze commits to upgrading to a Business-tier Lovable plan no later than its first paying customer, at which point Lovable's DPA will apply under Lovable's standard terms and govern Lovable's processing of data on OfficeEaze's behalf as platform infrastructure provider.

1.8. "Processing" / "Process"

means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

1.9. "Processor"

means Lou Squared Systems Inc. operating as OfficeEaze — the party that processes Personal Data on behalf of the Controller.

1.10. "Service"

has the meaning given in the recitals and includes the platform, the Harris AI assistant, and all features accessible through the Customer's OfficeEaze account.

1.11. "Sub-Processor"

means any third party engaged by OfficeEaze to Process Personal Data on OfficeEaze's behalf in connection with the Service. The current list of Sub-Processors is set out in Schedule B.

1.12. "Terms of Service"

means the OfficeEaze Terms of Service agreement between the parties, as updated from time to time, which governs the Customer's use of the Service.

Section 2 — Scope and Purpose of Processing

2.1 Instructions

OfficeEaze shall Process Personal Data only on documented instructions from the Customer, as set out in this Agreement and the Terms of Service. The Customer's use of the Service constitutes documented instructions to Process Personal Data for the purposes described in Schedule A. OfficeEaze shall immediately notify the Customer if, in OfficeEaze's reasonable opinion, any instruction from the Customer would violate Applicable Privacy Law.

2.2 Nature and Purpose of Processing

The nature, purpose, types of Personal Data, and categories of Data Subjects are described in Schedule A.

2.3 Duration

OfficeEaze shall Process Personal Data for the duration of the Customer's subscription and for such additional periods as required for compliance with legal retention obligations under Section 11.

2.4 Limitation of Purpose

OfficeEaze shall not Process Personal Data for any purpose other than:

- (a) providing and maintaining the Service as described in the Terms of Service;
- (b) complying with its legal obligations under Applicable Privacy Law or other applicable law;
- (c) anonymizing or aggregating Personal Data in a form that cannot reasonably be used to identify any individual, for the purpose of product improvement or analytics — provided that such anonymized data cannot be re-identified; and
- (d) such other purposes as the Customer may specifically authorize in writing.

OfficeEaze shall not use Personal Data to train artificial intelligence or machine learning models, sell Personal Data to third parties, share Personal Data for advertising purposes, or disclose Personal Data to any third party except as permitted under Section 5.

Section 3 — Obligations of OfficeEaze as Processor

3.1 Confidentiality

OfficeEaze shall ensure that any person authorized to Process Personal Data is subject to a binding confidentiality obligation. OfficeEaze shall maintain this obligation for the duration of this Agreement and after its termination.

3.2 Security Measures

OfficeEaze shall implement and maintain appropriate technical and organizational security measures to protect Personal Data. These measures shall include at minimum:

- (a) AES-256-GCM encryption of Personal Data at rest, with separate encryption keys per data category (Social Insurance Numbers, banking details, dates of birth, and medical information are each encrypted with dedicated keys);
- (b) TLS 1.3 or equivalent encryption of Personal Data in transit;
- (c) Row-level security ensuring complete data isolation between all customer accounts;
- (d) Mandatory two-factor authentication for all employer accounts;
- (e) Passkey (WebAuthn/FIDO2) authentication support for Face ID and fingerprint sign-in;
- (f) Automatic session expiration after 30 minutes of inactivity;
- (g) Immutable audit logging of all access to Personal Data with timestamp, user identity, and IP address;
- (h) Role-based access controls limiting team member access on a need-to-know basis;

- (i) Physical and logical access controls restricting production system access to authorized OfficeEaze personnel only;
- (j) Wiz SAST security scanning on all code deployments; and
- (k) Platform infrastructure provided by Lovable Inc., which maintains SOC 2 Type II and ISO 27001:2022 certifications and publishes a subprocessor list. Lovable's published Data Processing Agreement is included automatically for customers on Lovable's Business or Enterprise plan tier; OfficeEaze is currently on Lovable's Pro plan and commits to upgrading to a Business-tier plan no later than its first paying customer, at which point that DPA will apply. See Schedule C.

3.3 Assistance with Data Subject Rights

OfficeEaze shall assist the Customer by appropriate technical and organizational measures in fulfilling obligations to respond to Data Subject requests including rights of access, correction, deletion, withdrawal of consent, and data portability. Contact privacy@officeeaze.ca. OfficeEaze shall respond within five (5) business days.

3.4 Assistance with Legal Obligations

OfficeEaze shall assist the Customer in ensuring compliance with obligations under Applicable Privacy Law including security of processing, Data Breach notification, privacy impact assessments, and prior consultation with regulatory authorities.

3.5 Records of Processing

OfficeEaze shall maintain written records of all categories of Processing activities carried out on behalf of the Customer, to the extent required under Applicable Privacy Law. These records shall be made available to the Customer and regulatory authorities upon request.

3.6 Harris AI Assistant — Specific Restrictions

Where the Customer uses the Harris AI assistant, the following restrictions apply:

- (a) Harris shall not be provided with, or have access to, any employee's Social Insurance Number, banking or direct deposit information, date of birth, or medical information;
- (b) Inputs to Harris shall be limited to anonymized business context, aggregated metrics, and non-sensitive operational data as described in Schedule A;
- (c) Harris AI responses are generated using the Anthropic API. Anthropic does not use API data to train its models, as confirmed in Anthropic's API terms. Lovable's published Data Processing Agreement (Section 10.1) separately prohibits use of Customer Personal Data for AI/ML training at the infrastructure level once it applies to OfficeEaze's plan; and
- (d) The Customer may disable the Harris AI feature at any time through their account settings. Harris memory (pattern memory, payroll notes, bookkeeping notes, and HR notes) is stored in the Customer's OfficeEaze database and can be deleted at any time from Settings → Harris Memory.

3.7 Dedicated Tenant Environments

Where the Customer's account has been designated as a Dedicated Tenant Environment by OfficeEaze (as confirmed in the Customer's order documentation or enterprise agreement), the following additional provisions apply:

- (a) Physical isolation — the Customer's Personal Data shall be stored in a dedicated database instance provisioned exclusively for the Customer, hosted in the AWS ca-central-1 region (Montreal, Quebec, Canada). The Customer's Personal Data shall not share database

infrastructure with any other OfficeEaze customer;

(b) Dedicated credentials — the Customer's dedicated environment shall have its own isolated API keys, storage bucket, and authentication configuration. No credentials are shared with any other customer environment;

(c) Breach scope limitation — in the event of a Data Breach, the physical isolation of the Customer's environment means that a breach affecting another OfficeEaze customer's environment cannot expose the Customer's Personal Data, and vice versa. OfficeEaze shall confirm the scope of any breach in its notification under Section 6.1;

(d) Termination and migration — upon termination of the Customer's enterprise agreement, OfficeEaze shall provide the Customer with a complete export of all Personal Data from the dedicated environment in a structured, machine-readable format prior to decommissioning the environment. Decommissioning shall include secure deletion of all Personal Data and confirmation in writing; and

(e) Standard accounts — where the Customer's account has not been designated as a Dedicated Tenant Environment, Personal Data is protected by logical isolation through row-level security as described in Section 3.2(c), and all other provisions of this Agreement apply in full.

Section 4 — Obligations of the Customer as Controller

4.1 Lawful Basis

The Customer shall ensure that it has a valid lawful basis under Applicable Privacy Law for collecting and processing Personal Data about Data Subjects and for instructing OfficeEaze to Process such data on its behalf.

4.2 Consent and Notice

The Customer shall be responsible for: (a) providing all required notices and disclosures to Data Subjects; (b) obtaining all required consents prior to entering Personal Data into the Service; and (c) ensuring that the purposes for which Personal Data is entered are consistent with consents and notices provided to Data Subjects.

4.3 Accuracy

The Customer shall be responsible for the accuracy, quality, and legality of all Personal Data entered into the Service.

4.4 Authorized Users

The Customer shall ensure that access to Personal Data within the Service is restricted to authorized users with a legitimate need. The Customer shall promptly revoke access for any user who is no longer authorized.

4.5 Background Checks

Where the Customer uses the background check feature, the Customer represents and warrants that it has obtained the express informed consent of each candidate prior to initiating any background check, as required by Applicable Privacy Law and applicable provincial consumer reporting legislation.

4.6 Selfie Clock-In

Where the Customer enables selfie clock-in for employees, the Customer represents and warrants that it has obtained informed consent from each employee whose photograph will be captured, in compliance with applicable privacy legislation.

Section 5 — Sub-Processors

5.1 Authorized Sub-Processors

The Customer hereby provides general authorization for OfficeEaze to engage Sub-Processors to assist in providing the Service. The current list of authorized Sub-Processors is set out in Schedule B.

5.2 Sub-Processor Obligations

Where OfficeEaze engages a Sub-Processor to Process Personal Data, OfficeEaze shall: (a) impose data protection obligations equivalent in substance to those in this Agreement; (b) remain liable for the Sub-Processor's performance; and (c) ensure the Sub-Processor provides sufficient guarantees to implement appropriate technical and organizational measures.

5.3 Changes to Sub-Processors

OfficeEaze shall provide the Customer with at least thirty (30) days written notice before adding any new Sub-Processor or making any material change to an existing Sub-Processor's role. Notice shall be provided by updating officeeaze.ca/subprocessors and sending an email notification to the Customer's account email address.

If the Customer objects to a new or changed Sub-Processor on reasonable privacy or security grounds, the Customer shall notify OfficeEaze within twenty (20) business days of receiving notice. The parties shall work together in good faith to resolve the objection. If unresolved, the Customer may terminate this Agreement on thirty (30) days written notice without penalty, and OfficeEaze shall provide a pro-rated refund of any prepaid subscription fees.

Legal note — The twenty (20) business day objection window aligns with Section 7.3 of Lovable's published Data Processing Agreement, ensuring OfficeEaze can fulfill its upstream obligations within the Customer's objection period once that DPA applies to OfficeEaze's plan.

5.4 Cross-Border Transfers

The Customer acknowledges that certain Sub-Processors (including Anthropic PBC, Resend Inc., Twilio Inc., and Cloudflare Inc.) are located in the United States and may process limited Personal Data outside Canada. OfficeEaze confirms that:

- (a) Sensitive Personal Data including Social Insurance Numbers, banking details, dates of birth, and medical information is not transmitted to any Sub-Processor located outside Canada in plain text;
- (b) Data processed by US-based Sub-Processors is limited to: email addresses and notification content (Resend), mobile phone numbers and authentication codes only (Twilio), anonymized company context for AI responses (Anthropic), and security and routing data (Cloudflare);
- (c) All primary customer data including employee records, payroll data, and documents is stored in the AWS ca-central-1 region (Montreal, Quebec, Canada); and
- (d) Each US-based Sub-Processor is bound by contractual data protection obligations and holds the certifications described in Schedule B.

Section 6 — Data Breach Notification

6.1 OfficeEaze Notification

In the event of a Data Breach, OfficeEaze shall:

- (a) notify the Customer without undue delay, and in any event within seventy-two (72) hours of becoming aware of the Data Breach;
- (b) provide, to the extent available: (i) the nature of the Data Breach including categories and approximate number of Data Subjects affected; (ii) categories and approximate number of Personal Data records affected; (iii) the likely consequences; and (iv) measures taken or proposed to address the Data Breach;
- (c) cooperate with the Customer and take reasonable steps to investigate, contain, and remediate the Data Breach; and
- (d) not make any public disclosure identifying the Customer or its employees without the Customer's prior written consent, except as required by law.

6.2 Customer Notification

The Customer is responsible for determining whether the Data Breach triggers a notification obligation to the Office of the Privacy Commissioner of Canada under PIPEDA's mandatory breach reporting requirements. OfficeEaze shall provide reasonable assistance upon request.

6.3 Remediation

OfficeEaze shall promptly take all reasonable steps to remediate any Data Breach and prevent recurrence, and shall provide the Customer with a written incident report within thirty (30) days of containing the breach.

6.4 Platform Breach

Where a Data Breach originates at the Lovable Inc. platform infrastructure level, OfficeEaze shall notify the Customer as soon as Lovable notifies OfficeEaze, consistent with the breach notification obligations in Section 6 of Lovable's published Data Processing Agreement.

Section 7 — Data Residency and Canadian Storage

7.1 Primary Storage

OfficeEaze confirms that all Personal Data described in Schedule A is stored in the Amazon Web Services ca-central-1 region (Canada Central — Montreal, Quebec). OfficeEaze shall not migrate primary storage of Personal Data outside Canada without: (a) providing the Customer with at least sixty (60) days advance written notice; (b) conducting a Transfer Impact Assessment; and (c) implementing appropriate safeguards.

7.2 Infrastructure Certification

The platform infrastructure on which OfficeEaze operates is provided by Lovable Inc. Lovable maintains SOC 2 Type II and ISO 27001:2022 certifications. Lovable's published Data Processing Agreement — which under Section 5.2 obliges Lovable to maintain those accreditations — is included automatically for customers on Lovable's Business or Enterprise plan tier. OfficeEaze currently operates on Lovable's Pro plan and has not itself separately executed a DPA with Lovable; OfficeEaze commits to upgrading to a Business-tier Lovable plan no later than its first

paying customer, at which point Lovable's DPA will apply under Lovable's standard terms. Current compliance documentation is available on request — contact privacy@officeeaze.ca.

7.3 Canadian Law Governs

This Agreement is governed by the laws of the Province of Ontario and the laws of Canada applicable therein. Both parties irrevocably attorn to the exclusive jurisdiction of the courts of Ontario for any dispute arising under this Agreement.

Section 8 — Audits and Inspections

8.1 Audit Rights

OfficeEaze shall, upon reasonable written request (with no less than thirty (30) days notice), make available to the Customer all information reasonably necessary to demonstrate compliance with this Agreement, including:

- (a) current security certifications and reports (SOC 2 Type II report, ISO 27001 certificate, penetration test attestation) subject to confidentiality obligations — available on request through privacy@officeeaze.ca;
- (b) a summary of the most recent annual penetration test of the OfficeEaze application layer (Q3 2026 onwards); and
- (c) a completed privacy and security questionnaire reasonably requested by the Customer.

8.2 Limitations

Audit requests shall not unreasonably interfere with OfficeEaze's operations and shall not require disclosure of other customers' Personal Data. The Customer shall bear the costs of any audit it requests unless the audit reveals a material breach of this Agreement by OfficeEaze.

Section 9 — Data Subject Rights and Privacy Requests

9.1 Forwarding Requests

If OfficeEaze receives a request directly from a Data Subject exercising rights under Applicable Privacy Law, OfficeEaze shall promptly forward the request to the Customer without responding directly, unless legally required to respond. The Customer is responsible for responding to all Data Subject requests.

9.2 Assistance

OfficeEaze shall provide reasonable technical assistance to the Customer in responding to Data Subject requests, including data extracts, access logs, and other information reasonably required to fulfill rights of access or correction.

9.3 Right to Erasure

Where a Data Subject requests erasure of their Personal Data, the Customer shall determine whether any legal retention obligation applies. OfficeEaze shall execute erasure as instructed, subject to Section 11.

Section 10 — Employee Data — Special Obligations

10.1 Sensitivity of Employee Data

The parties acknowledge that Personal Data processed under this Agreement includes highly sensitive information including Social Insurance Numbers, banking details, compensation history, and medical information. Both parties agree to treat this category of data with heightened care consistent with the principles of data minimization, purpose limitation, and storage limitation under Applicable Privacy Law.

10.2 SIN Handling and Platform DPA Interaction

Social Insurance Numbers are government identifiers. OfficeEaze ensures that Social Insurance Numbers are:

- (a) encrypted using a dedicated AES-256-GCM encryption key before storage in the OfficeEaze application database (AWS ca-central-1, Montreal);
- (b) displayed in masked format (XXX-XXX-XXXX) in all user interfaces by default;
- (c) only decrypted and displayed in full after the employer re-authenticates within the current session;
- (d) logged each time they are accessed, including the accessing user's identity and timestamp; and
- (e) never transmitted to any Sub-Processor, including the Harris AI assistant or Lovable's platform layer, in plain text.

OfficeEaze's position is that, because Social Insurance Numbers are encrypted at the application layer within Supabase/AWS before reaching Lovable's infrastructure, they do not pass through Lovable's platform in a form that constitutes "providing" sensitive data to Lovable within the meaning of Section 3.8 of Lovable's published Data Processing Agreement (which restricts providing data classified as sensitive, including 'government identifiers,' to Lovable). That DPA applies to customers on Lovable's Business or Enterprise plan tier; OfficeEaze is currently on Lovable's Pro plan and will be covered on upgrade to a Business-tier plan, which OfficeEaze commits to no later than its first paying customer. This interpretation has not yet been independently confirmed by outside legal counsel.

10.3 Banking Details

Employee direct deposit and banking details shall be encrypted with a dedicated encryption key separate from the SIN key, decrypted only server-side when generating payroll files, and never displayed in plain text except to the account owner or authorized payroll administrator.

10.4 Medical Information

Medical information entered into the Service shall be encrypted at rest, accessible only to users with explicit HR permissions, and never transmitted to the Harris AI assistant.

Section 11 — Data Retention and Deletion

11.1 Retention During Service

OfficeEaze shall retain Personal Data for the duration of the Customer's subscription and for any additional period required by law as set out in Section 11.2.

11.2 Legal Retention Requirements

The following retention periods apply after termination of the Customer's account:

- (a) Payroll records, T4 slips, and employment tax records — minimum six (6) years after the end of the tax year (Income Tax Act, Canada);
- (b) Records of Employment — six (6) years (Employment Insurance Act);
- (c) Employment agreements and HR records — six (6) years or applicable limitation period;
- (d) Invoices and financial records — six (6) years (Income Tax Act, Canada); and
- (e) Security and audit logs of sensitive data access — three (3) years.

11.3 Deletion on Termination

Upon expiration of each applicable retention period, OfficeEaze shall securely delete or anonymize the relevant Personal Data using industry-standard deletion methods. OfficeEaze shall confirm deletion in writing upon request.

Note: Under Section 11.2 of Lovable's published Data Processing Agreement, following termination of OfficeEaze's agreement with Lovable, the Customer may instruct OfficeEaze within thirty (30) calendar days to return or delete Customer Personal Data. OfficeEaze will pass through this instruction to Lovable as required.

11.4 Customer-Initiated Deletion

The Customer may request deletion of specific Personal Data at any time by contacting privacy@officeeaze.ca. OfficeEaze shall action deletion requests within thirty (30) days, subject to any legal retention obligation under Section 11.2.

11.5 Data Export

At any time during the subscription, the Customer may export all of its Personal Data in a structured, machine-readable format through Settings → Export Your Data. OfficeEaze shall not charge any fee for data export.

Section 12 — Privacy Officers

12.1 OfficeEaze Privacy Officer

OfficeEaze Privacy Officer: Nadine Leduc — Co-Founder and Privacy Officer

Email: privacy@officeeaze.ca

Mailing address: 18 Joe Taylor Lane, Carbonear, NL A1Y1A9 (Privacy Officer mailing address)

Registered office of Lou Squared Systems Inc.: 158 Day Road, Castleton, Ontario K0K 1M0

12.2 Customer Privacy Contact

The Customer shall designate a primary contact for privacy matters. All breach notifications, sub-processor change notices, and legal requests shall be sent to the Customer's account email address unless the Customer designates a separate privacy contact in writing.

Section 13 — Liability

13.1 OfficeEaze Liability

OfficeEaze shall be liable to the Customer for direct damages arising from OfficeEaze's breach of this Agreement, subject to the limitation of liability provisions in the Terms of Service.

13.2 Customer Liability

The Customer shall indemnify OfficeEaze against any claims, penalties, or regulatory proceedings arising from: (a) failure to obtain valid consent from Data Subjects; (b) failure to comply with obligations as data controller under Applicable Privacy Law; (c) instructions given by the Customer that violate Applicable Privacy Law; and (d) inaccurate, incomplete, or unlawful Personal Data entered into the Service.

13.3 Third-Party Claims

Each party shall promptly notify the other of any complaint, claim, or regulatory proceeding by a third party relating to the processing of Personal Data. The parties shall cooperate in good faith in responding.

Section 14 — Regulatory Cooperation

Where the Office of the Privacy Commissioner of Canada or any provincial privacy commissioner undertakes an investigation relating to Personal Data processed under this Agreement, the parties shall: (a) promptly notify each other; (b) cooperate in good faith with the regulator; (c) keep each other reasonably informed of the status; and (d) not make any admission of liability or offer of settlement that binds the other party without prior written consent.

Section 15 — Term and Termination

15.1 Term

This Agreement commences on the date of execution and continues for the duration of the Customer's subscription and thereafter for the legal retention periods in Section 11.

15.2 Termination for Breach

Either party may terminate this Agreement for material breach upon thirty (30) days written notice if the breach is not remedied within that period.

15.3 Effect of Termination

Upon termination: (a) OfficeEaze shall cease all Processing of Personal Data except as required for legal retention obligations; (b) the Customer shall have thirty (30) days to export all data through Settings → Export Your Data; and (c) OfficeEaze shall confirm in writing the deletion of all Personal Data upon completion of applicable retention periods.

Section 16 — Confidentiality of Agreement

The terms of this Agreement are confidential. Neither party shall disclose the terms to any third party without the other party's prior written consent, except: (a) to legal counsel or professional advisors under a duty of confidentiality; (b) as required by applicable law or court order; or (c) in connection with enforcement of this Agreement.

Section 17 — General Provisions

17.1 Entire Agreement — This Agreement, together with the Terms of Service and all Schedules, constitutes the entire agreement between the parties with respect to processing of Personal Data.

17.2 Relationship to Terms of Service — In the event of conflict with respect to processing of Personal Data, this Agreement prevails.

17.3 Amendment — This Agreement may only be amended by written instrument signed by authorized representatives of both parties, except that OfficeEaze may update the Sub-Processor list in Schedule B in accordance with Section 5.3.

17.4 Severability — If any provision is found invalid, it shall be modified to the minimum extent necessary. Remaining provisions continue in full force.

17.5 No Waiver — Failure to exercise any right under this Agreement shall not constitute a waiver.

17.6 Counterparts — This Agreement may be signed in counterparts. Electronic signatures are valid and binding.

17.7 Language — The parties confirm their express wish that this Agreement be drawn up in the English language. Les parties confirment leur volonté expresse que la présente entente soit rédigée en langue anglaise.

Section 18 — Changes to This Agreement

OfficeEaze may update this Agreement from time to time. Material changes will be communicated by email with at least fourteen (14) days notice and will require renewed acceptance before continued use of the Service.

Signatures

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the date first written above.

Lou Squared Systems Inc. operating as OfficeEaze (Processor)

Signature: _____

Name: _____

Title: _____

Date: _____

On behalf of: _____

[CUSTOMER LEGAL NAME] (Controller)

Signature: _____

Name: _____

Title: _____

Date: _____

On behalf of: _____

Schedule A — Description of Processing

A.1 Subject Matter

Processing of personal information about the Customer's employees, contractors, and job applicants in connection with payroll, HR management, employee onboarding, scheduling, and

related business operations.

A.2 Duration

For the duration of the Customer's subscription and the legal retention periods in Section 11.

A.3 Nature of Processing

Collection, storage, organization, retrieval, use, disclosure to authorized users, encryption, and deletion of Personal Data as described below.

A.4 Purposes of Processing

- Processing payroll including CPP, EI, and income tax deductions
- Generating pay stubs, T4 slips, T5 slips, and Records of Employment
- Managing employee onboarding including digital TD1 forms and policy signing
- Storing employment agreements, HR records, and performance reviews
- Processing direct deposit and banking information for payroll disbursement
- Managing employee scheduling, time tracking, and attendance
- Processing expense claims and reimbursements
- Generating compliance documents
- Maintaining a digital filing cabinet for employment-related documents
- Providing AI-assisted business operations through the Harris assistant using anonymized business context only — see Section 3.6

A.5 Categories of Personal Data

Category 1 — Identity Data (Sensitive):

Full legal name, date of birth (encrypted), Social Insurance Number (encrypted with dedicated key), home address, emergency contact information

Category 2 — Financial Data (Sensitive):

Banking institution number, transit number, and account number (encrypted with dedicated key), compensation history, T4/T5/ROE data, expense records

Category 3 — Employment Data:

Employment dates, job title, department, employment type, work schedule, hours worked, performance reviews, training records, disciplinary records, leave records

Category 4 — Medical Data (Sensitive — where entered):

Medical leave reasons, disability and accommodation information, workplace injury and WCB claim information

Category 5 — Authentication Data:

Email address, mobile phone number (for SMS authentication), passkey public keys (per device), authentication tokens (encrypted)

Category 6 — Harris AI Input (Non-Sensitive):

Company name and province, aggregated payroll metrics (no individual employee data), CRA remittance amounts and deadlines, Harris memory (pattern memory, payroll notes, bookkeeping

and HR notes stored in OfficeEaze database)

A.6 Categories of Data Subjects

- Current and former employees of the Customer
- Contractors and independent service providers
- Job applicants (background check module only, with consent)
- Account owner and authorized team members of the Customer

A.7 Data Not Processed

OfficeEaze does not process and the Customer must not enter: credit card or payment card numbers of employees, passport or immigration document numbers other than SIN, or personal data of individuals under 18 except as required for lawfully employed young workers with proper consent.

Schedule B — Authorized Sub-Processors

Current as of May 2026. Updates provided per Section 5.3. Full public list at officeeaze.ca/subprocessors.

1. Lovable Inc. — Application hosting and platform infrastructure

Location: Canada (AWS ca-central-1, Montreal) + United States

Data: All customer data via AWS infrastructure (application layer)

Certifications: SOC 2 Type II (contractual commitment), ISO 27001 (contractual commitment)

DPA: Lovable's published Data Processing Agreement, included automatically for customers on Lovable's Business or Enterprise plan tier. OfficeEaze is currently on Lovable's Pro plan and has not separately executed a DPA with Lovable; coverage applies on upgrade to a Business-tier plan, which OfficeEaze commits to no later than its first paying customer. In the interim OfficeEaze relies on Lovable's SOC 2 Type II and ISO 27001:2022 certifications and published subprocessor list.

Compliance documentation: available on request — privacy@officeeaze.ca

2. Amazon Web Services — Cloud infrastructure

Location: Canada (ca-central-1 — Montreal, Quebec)

Data: Customer records, employee data, documents, payroll records

Certifications: SOC 2 Type II, ISO 27001, CSA STAR

3. Anthropic PBC — Harris AI assistant

Location: United States

Data: Anonymized company context ONLY — no SINS, banking details, employee names, or personal data

AI training: Anthropic does not use API data to train models

4. Helcim Inc. — Payment processing

Location: Canada (Calgary, Alberta)

Data: Billing name, email, subscription payment data — no employee personal data

Certifications: PCI DSS Level 1

5. Resend Inc. — Transactional email delivery

Location: United States

Data: Email address and notification content only — no sensitive personal data

Certifications: SOC 2 Type II

6. Twilio Inc. — SMS authentication

Location: United States

Data: Mobile phone number and 6-digit authentication code ONLY

Certifications: ISO 27001, SOC 2 Type II

7. Cloudflare Inc. — Security and CDN

Location: Global CDN

Data: Request routing metadata and security logs — no Personal Data content

Certifications: SOC 2 Type II, ISO 27001

8. Google LLC — Gmail receipt scanning (optional — only if enabled by Customer)

Location: United States | Certifications: ISO 27001, SOC 2 Type II

9. Microsoft Corporation — Outlook receipt scanning (optional — only if enabled by Customer)

Location: United States | Certifications: ISO 27001, SOC 2 Type II

10. ElevenLabs Inc. — Harris voice interface (optional — only if used by Customer)

Location: United States | Data: Voice audio only — no Personal Data content

Schedule C — Platform Data Protection and Security Standards

C.1 Lovable Inc. — Platform Data Processing Agreement status

Lovable Inc. (Lovable Labs Incorporated, 1111b South Governors Avenue, Dover, DE 19904) publishes a Data Processing Agreement that, under Lovable's own terms, is included automatically for customers on Lovable's Business or Enterprise plan tier:

Current status: OfficeEaze operates on Lovable's Pro plan. OfficeEaze has not itself separately executed a DPA with Lovable.

Planned coverage: OfficeEaze commits to upgrading to a Business-tier Lovable plan no later than its first paying customer, at which point Lovable's DPA will apply under Lovable's standard terms.

Interim reliance: Lovable's SOC 2 Type II and ISO 27001:2022 certifications and its published subprocessor list.

Data Protection Officer: Annabel Pemberton — dpo@lovable.dev

Sub-processor list: enterprise.lovable.dev/subprocessors

Key provisions of Lovable's published Data Processing Agreement relevant to this Agreement once it applies:

Section 5.2 — Lovable shall maintain SOC 2 Type II and ISO 27001 accreditations for the duration of the agreement

Section 6 — Breach notification without undue delay, with investigation and root cause identification

Section 10.1 — Lovable shall not use Customer Personal Data for AI or ML model training

Section 11.2 — Data return or deletion within 30 calendar days of agreement termination

Section 7.3 — Customer (OfficeEaze) may object to new sub-processors within 20 business days

C.2 Section 3.8 — Government Identifiers

Section 3.8 of Lovable's published Data Processing Agreement states that the customer shall not provide 'government identifiers' to Lovable. Social Insurance Numbers are government identifiers. OfficeEaze's technical position is that SINs are encrypted at the application layer within AWS ca-central-1 using a dedicated AES-256-GCM key before reaching any layer of Lovable's platform infrastructure, and therefore SINs do not pass through Lovable's systems in a form that constitutes 'providing' government identifier data to Lovable within the meaning of Section 3.8. This interpretation has not yet been independently confirmed by outside legal counsel.

C.3 OfficeEaze Application Security

- AES-256-GCM encryption at rest with dedicated keys per data category
- TLS 1.3 encryption in transit
- Row-level security on all database tables
- Mandatory TOTP two-factor authentication for all employer accounts
- Passkey (WebAuthn/FIDO2) authentication — Face ID and fingerprint support
- Automatic 30-minute inactivity session expiry
- Immutable audit logging of all sensitive data access
- IP-based and account-based rate limiting on authentication endpoints
- Wiz SAST security scanning on all code deployments
- Random UUID storage paths for all uploaded files
- Server-side MIME type validation for all file uploads

C.4 Planned Security Enhancements

- Independent third-party penetration test of OfficeEaze application layer — scheduled Q3 2026. Results summary will be published at officeeaze.ca/security.

C.5 Incident Response

- 72-hour breach notification to affected customers
- Designated security contact: security@officeeaze.ca
- Post-incident review and remediation report within 30 days of containment