Version: 2.2
Last Updated: 1st May 2026

SECLORE-CONTROLLER-PROCESSOR DATA PROCESSING ADDENDUM

This Controller-Processor Data Processing Addendum ("**DPA**") amends and/or is deemed fully incorporated into the AI Terms (*together with any amendments, software subscription agreements, statements of work, attachments, schedules, exhibits, and/or order forms* between the Customer and Seclore, *the "**Agreement**"*).

This DPA governs the Processing (defined below) of certain Personal Data (defined below) by Seclore on behalf of the Customer, in accordance with applicable laws, and encompasses all activities related to the provision of Services under the Agreement. It includes, in conjunction with the Agreement, documented instructions, specifying the subject-matter, duration, nature, and purpose of the Processing, and establishing the rights and obligations of the Parties.

The Agreement is the Customer's complete instructions to Seclore for the Processing of Personal Data.

1. Definitions and interpretation:

"Authorized Users"	means any individuals whom the Customer authorized to access and use the Services and/or Software and who has been given a unique user identification by Customer, or an individual whom the Customer authorized to sign any agreements with Seclore;
"Customer"	has the meaning set out in the Agreement;
"Data Controller"	means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data*. For the purposes of this DPA, the Data Controller shall be the Customer;*
"Data Processor"	means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. *For the purposes of this DPA, the Data Processor shall be Seclore and any other third parties to which the Processing was delegated by Seclore;*
"Data Protection Regulations"	means any applicable laws, regulations, or other legal requirements relating to the Processing of Personal Data and/or privacy, including but not limited to GDPR, CCPA, the Colorado Privacy Act, the Connecticut Privacy Act, the Virginia Consumer Data Protection Act, their implementing regulations, and similar laws;
"Data Subject"	means the Identified or Identifiable Natural Person to whom the Personal Data relates;
"CCPA"	means California Consumer Privacy Act (as amended), Cal. Civ. Code §§ 1798.100 et seq. including any amendments and implementing regulations that become effective on or after the effective date of this DPA;
"EEA"	means the European Economic Area as defined under the GDPR;
"**File Data**"	means the information stored by Seclore as part of the Services, and is limited to: (i) full name of Users and External Users; (ii) e-mail ID of Users and External Users; (iii) user ID of Users and External Users; (iv) Internet Protocol address of Users and External Users, (v) machine details of Users and External Users; (vi) activity date of Users and External

	Users; (vii) password of External Users; (viii) File ID; and (ix) File Name, File permissions, encryption keys and activity logs of the Users and External users (which documents the Files accessed by a User and/or External User and actions performed by said User and/or External User on each File).
"GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the European Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
"Identified or Identifiable Natural Person"	means a natural person (individual) who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person;
"Personal Data"	means any information relating to an Identified or Identifiable Natural Person, and for the purposes of the Agreement, this term includes (without limitation) any Personal Data Processed by Seclore as a result of entering into or performing its obligations under the Agreement and any associated documents;
"Process", "Processed" or "Processing"	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;
"Seclore"	has the meaning set out in the Agreement;
"Services"	means the services specified under the Order Form;
"Sub-Processor"	means any third-party engaged by Seclore under this Agreement for Processing Personal Data on behalf of Seclore including without limitation the sub-processors more particularly described in Annex III.
"Supervisory Authority"	means any government authority or public body acting on behalf of any government authority under applicable laws.

Unless otherwise defined above, all capitalized terms used in this DPA will have the meaning given to them under the Agreement.

The terms and conditions of this DPA shall, in the event of conflict or inconsistency with any other privacy-related documents, including privacy policies or privacy notices, take precedence over such documents.

2. Data Processing

2.1. Seclore will Process Personal Data for the duration of the Agreement unless a different timetable is agreed upon by the Parties in writing or as required by applicable law.

2.2. The Parties acknowledge and agree that with regard to the Processing of Personal Data on behalf of the Customer, the details specified under Annex I shall apply. The Customer is the Controller and Seclore is a Processor to the extent it Processes Personal Data.

2.3. The Customer is responsible for the accuracy, quality, and legality of the Personal Data Processed by Seclore, and the means by which the Customer acquired the Personal Data, including but not limited to procuring any necessary consents from Data Subjects, including any third-party Data Subjects, as required by Section 2.4.4.

2.4. Any Processing of Personal Data by Seclore under this DPA shall occur only:

2.4.1. on behalf of and upon authorization from the Customer (including through its Authorized Users);

2.4.2. in accordance with the Agreement;

2.4.3. for the purpose of fulfilment of the Customer's written instructions; and

2.4.4. where required under Data Protection Regulations or other applicable laws, upon the Customer procuring valid consent from the Data Subjects for such Processing.

2.5. The types of Personal Data affected by the Processing within the scope of this DPA may include:

(a) Authorized User's name and email address;

(b) Authorized User's Internet Protocol (IP) addresses;

(c) Device name and Security Identifier (SID);

(d) Login identification;

(e) Authorized User agent type;

(f) Operating system;

(g) Date/time stamp of usage and activities performed with the Customer's file (such as access and close times and metadata);

(h) Authorized User's device ID;

(i) Authorized User's folder name; and

(j) File Data (which may include such personal datasets that the Customer may choose to provide from time to time).

2.5.1. In case any Personal Data is stored within the Customer's files, such data is stored temporarily in Seclore's servers solely to carry out the Services.

2.6. Personal Data may be subject to the following basic Processing activities:

2.6.1. For the provision of the Services contemplated under the Agreement (which includes (a) enabling the Customer to control and monitor information in the form of documents, emails, designs, and images, (b) using Seclore's AI models to classify and label Customer Data, and (c) generating suggestions and recommendations for the Customer);

2.6.2. For installation of the Services and creation of Authorized User accounts, and to provide access to the Services;

2.6.3. For analyzing aggregate usage patterns and trends; and

2.6.4. For monitoring compliance with the terms of this Agreement.

2.7. The categories of Data Subjects affected by the Processing of Personal Data on behalf of the Customer within the scope of this DPA will include:

2.7.1. Customer's employees and personnel designated as Authorized Users; and

2.7.2. Customer's prospects, clients, business partners, vendors, associates, consultants, agents, and their respective personnel, and such other persons whose Personal

Data may be included in the Customer's files.

2.8. Sensitive and Special categories of data: The Parties acknowledge that Seclore will not intentionally collect or Process sensitive or special categories of Personal Data, such as personal health information or individualized payment data, unless instructed to do so by the Customer.

The Parties agree that the Customer shall be solely responsible for compliance with any Data Protection Regulations as applicable to Controllers, including for any Personal Data that requires special handling, or special categories of Personal Data, such as, without limitation, those which relate to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, or personal finances.

2.9. Duration of Processing:
Between Seclore and the Customer, the duration of Processing will be determined by the Customer, unless otherwise required under applicable laws. However, if the Customer doesn't specify the duration of Processing, Seclore shall retain the data for the Subscription Term unless earlier deletion or return is requested in writing by the Customer, or for the duration of time Seclore is required to Process the Personal Data pursuant to the Agreement or applicable Data Protection Regulations. Additionally, Seclore will retain the Personal Data for 90 days after the Subscription Term ends (the "**Holding Period**"). After the Holding Period expires, Seclore will destroy the data, or earlier upon the Customer's explicit written request.

3. General provisions:

3.1. Each Party will fully comply with all its obligations under the applicable Data Protection Regulations.

3.2. Seclore shall:

3.2.1. Process Personal Data only as necessary for the provision of Services required by the Agreement; and

3.2.2. act only in accordance with the lawful and documented instructions of the Customer.

3.3. Personnel:

3.3.1. The Parties shall:

(a) ensure all employees involved in the Processing or transferring of Personal Data have: (i) either committed themselves to confidentiality in writing or have statutory or fiduciary obligations requiring confidentiality; and (ii) are authorized by the respective Party and appropriately trained to Process Personal Data;

(b) ensure the access to Personal Data is limited to the personnel necessary to execute the Party's obligations under the Agreement; and

(c) appoint a data protection officer, if required by Data Protection Regulations, and provide their contact details on written request to the other Party.

3.4. Technical and Organizational Measures:

3.4.1. Seclore will take appropriate technical and organizational security measures against the accidental or unlawful Processing of Personal Data and against the accidental or unlawful loss, destruction, alteration, unauthorized disclosure of, or access to, Personal Data, as provided in Annex II. Seclore shall regularly test, assess, and evaluate the effectiveness of such technical and organizational measures in ensuring the security of the Processing.

3.5. Sub-Processing:

3.5.1. The Customer authorizes Seclore to engage Sub-Processors to fulfil its obligations under the Agreement.

3.5.2. Such Sub-Processors are listed in Annex III. Should Seclore wish to add to or replace such Sub-Processors, Seclore shall give the Customer reasonable notice and an opportunity to object, provided such objection is based on reasonable grounds relating to data protection. If the Customer does not object within thirty (30) days of the notice, or if the objection is not based on "reasonable grounds", then such added or replaced Sub-Processors shall be considered incorporated into Annex III as an amendment to this DPA.

3.5.3. Seclore shall impose substantially similar data protection obligations on any Sub-Processors as set out in this DPA (in particular, providing sufficient guarantees to implement appropriate technical and organizational measures). Seclore shall be liable for the acts and omissions of its Sub-Processors to the same extent Seclore would be liable if performing the Services of each Sub-Processor directly under the terms of this DPA.

3.6. Data Transfers:

3.6.1. Customer authorizes Seclore to store or Process Personal Data in the United States or any other country in which Seclore or its Sub-Processors maintain facilities, in order to provide the Services or to carry out documented instructions of the Customer. The Parties will conduct all such activities in compliance with the Agreement and applicable Data Protection Regulations.

3.7. U.S. Data Protection Regulations:

3.7.1. To the extent that Seclore Processes any Personal Data relating to individuals who are Californian residents, Seclore shall comply with the CCPA. For the purposes of the CCPA, the Parties agree that Seclore is a "Service Provider" in the performance of its obligations, and that the Customer is a "Business". As a Service Provider, Seclore shall not: (a) retain, use, or disclose any Personal Data: (i) for any purpose other than for the specific purpose of providing the Services specified in the Agreement, including for a commercial purpose other than providing the Services specified in the Agreement, (ii) outside of the direct business relationship between Seclore and the Customer, or (iii) as otherwise prohibited by the CCPA; or (b) sell

Personal Data. Finally, the transfer of any Personal Data to Seclore shall not be considered a "sale" as defined in the CCPA.

3.7.2. To the extent that Seclore Processes any Personal Data relating to individuals who are residents of any state in the United States besides California that has its own Data Protection Regulation, Seclore shall comply with those states' Data Protection Regulations.

3.8. Privacy Impact Assessment:

3.8.1. Taking into account the nature of the Processing, if the Customer reasonably believes or becomes aware that Seclore's Processing of Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects as prescribed under Data Protection Regulations, it shall promptly inform Seclore. Upon request and at the Customer's expense, Seclore shall use commercially reasonable efforts to provide the Customer with all such reasonable and timely assistance as the Customer may require in order to conduct a privacy impact assessment, and if necessary, consult with any relevant Supervisory Authority.

3.9. Rights of Data Subjects:

3.9.1. Seclore shall, to the extent permissible by Data Protection Regulations, promptly notify the Customer upon receipt of a request from a Data Subject to exercise any of the Data Subject's rights, including but not limited to the right of access, right to rectification, restriction of Processing, right to be forgotten, data portability, objection to Processing, or right not to be subject to automated individual decision-making. Taking into account the nature of the Processing, Seclore shall, to the extent feasible, assist the Customer in fulfilling its obligations to respond to the Data Subject's request through suitable technical and organizational measures.

3.10. Audits:

3.10.1. Seclore shall, at the Customer's expense, upon reasonable request of the Customer but only for cause (with approved causes set out in Section 3.10.3) and/or to the extent required by Data Protection Regulations, make available to the Customer all relevant information necessary for audits or inspections, conducted by the Customer or an independent auditor appointed by the Customer (subject to such auditor not being a competitor of Seclore and execution of a non-disclosure agreement) to demonstrate Seclore's compliance with its obligations under this DPA. Such audits or inspections shall be carried out only at Seclore's office premises and be limited to Seclore's Processing of Personal Data in its capacity as a Data Processor for the Customer only, and not any other aspect of Seclore's business or information systems or its other clients.

3.10.2. If the Customer requires Seclore to submit to audits or inspections, the Customer will provide Seclore with at least sixty (60) days' advance written notice of such audit or inspection. Such written notice will specify the things, people, places, or documents to be made available. Anything produced by Seclore during such audit or inspection will only be in connection with Seclore's engagement with the Customer and will not include any information pertaining to Seclore's other clients.

Further, such information produced for inspection will be considered Seclore's Confidential Information, and notwithstanding anything to the contrary in the Agreement, will remain Confidential Information in perpetuity or the longest time allowable by Data Protection Regulations after termination of the Agreement.

3.10.3. Seclore shall allow for onsite audit or inspection requests at the Customer's expense, only in cases where: (a) Seclore has not provided sufficient written evidence of its compliance with the technical and organizational measures, (b) a Security Breach has occurred, (c) an inspection is officially requested by the Customer's Supervisory Authority, or (d) Data Protection Regulations provide the Customer with a mandatory on-site inspection right, and provided that the Customer shall not exercise this right more than once per year unless Data Protection Regulations require more frequent inspections. Such facility inspections shall be conducted in a manner that does not impact the ongoing safety, security, commitments to other clients by Seclore, confidentiality, integrity, availability, continuity, and resilience of the inspected facilities, nor otherwise expose or compromise any confidential data Processed therein.

3.11. Security Breach

3.11.1. In the event of unauthorized or accidental use, disclosure or access of Personal Data or any other breach of this DPA by Seclore or any of its employees, Sub-Processors, or any other identified or unidentified third party ("**Security Breach**"), Seclore shall promptly notify the Customer in writing upon the discovery and confirmation of such Security Breach, without undue delay.

3.11.2. Such notification shall contain, at least:

(a) a description of the nature of the Security Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);

(b) the details of a point-of-contact where more information concerning the Personal Data breach can be obtained; and

(c) the likely consequences of, and the measures taken or proposed to be taken to address the Security Breach, including measures to mitigate its possible adverse effects.

3.11.3. Where, and insofar as, it is not possible to provide all the above information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

3.11.4. Seclore shall take all necessary and legally required corrective or mitigating actions, to remedy or mitigate any Security Breach; and

3.11.5. Seclore shall not make any announcement or publish or otherwise authorize any broadcast of any notice or information about the Security Breach without notifying the Customer, unless legally required to do so.

3.12. Cooperation with Supervisory Authorities:

3.12.1. In the event of reporting and notification obligations to Supervisory Authorities

and/or affected Data Subjects arising from Security Breaches, the Parties shall, upon request, extend reasonable support and furnish information to the other Party to facilitate the investigation of any Security Breach and to fulfil any legally mandated obligations.

4. Miscellaneous

4.1. This DPA may be amended, supplemented, or replaced by Seclore in written or otherwise documented form at any time by notifying the Customer through the email address provided by the Customer in the Agreement.

4.2. If Seclore cannot delete or return the Personal Data due to legal or regulatory requirements, Seclore will immediately inform the Customer and will take all necessary steps to ensure that the Personal Data concerned is kept confidential, subject to legal or regulatory requirements, and will not be further Processed.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The data exporter is the identified Controller in Section 1 of this DPA.

Data importer(s): The data importer is the Seclore entity identified as Processor in Section 1 of this DPA.

Address: Unit No 1002 and 1004, R Square, 10th Floor, Near J B Nagar Metro Station, Andheri Kurla Road, Bhim Nagar, Andheri East, Mumbai, Maharashtra 400059.

Email: DPO@seclore.com

Contact Details: Tuhina Chakrabarty, Director – Legal

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred:

1. Customer's employees / personnel designated as Authorized Users; and

2. Customer's prospects, clients, business partners, and vendors etc.

Categories of Personal Data transferred:

The types of Personal Data affected by the Processing within the scope of this DPA may include:

- Authorized User's name, email address;
- Authorized User's Internet Protocol (IP) addresses;
- Device name and Security Identifier (SID);
- Login identification;
- Authorized User agent type;
- Operating system;
- Date/time stamp of usage and activities performed with the Customer's files (access and close and metadata times);
- Authorized User's device ID;
- Authorized User's folder name; and
- File data (which may include such personal datasets that the Customer may choose to provide from time to time). In case any Personal Data is stored within the Customer's files, such data is stored temporarily in Seclore's servers solely to carry out the Services.

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 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:

As determined by the Customer.

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

As necessary for the purposes of Processing according to the Agreement.

Nature of the Processing:

Fulfilment of the purpose of the Agreement.

Purpose(s) of the data transfer and further Processing:

1. For the provision of the Services contemplated under the Agreement (which includes (a) enabling Customer to control and monitor information in the form of documents, emails, designs, and images (among other forms for conveying information), (b) Processing data using Seclore's AI models to classify and label files and documents, and (c) generating suggestions and recommendations to Customer);

2. For creation of Authorized User accounts and to provide access to Services;

3. For analysing aggregate usage patterns and trends; and

4. For monitoring compliance with the terms of this Agreement.

The period for which the Personal Data will be retained, or if that is not possible, the criteria used to determine that period:

Subject to Section 2 of the DPA, Seclore will retain Personal Data for as long as required for fulfilling the purposes under the Agreement, unless: (a) a longer retention period is required for audit, legal, or regulatory purposes; or (b) the Customer instructs Seclore in writing to: (i) keep certain Personal Data for longer, or (ii) return certain Personal Data earlier.

For transfers to (Sub-)Processors, also specify subject matter, nature, and duration of the Processing:

See Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: Data Protection Authority in Ireland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

This Annex describes the technical and organizational measures implemented by the **Processor** to protect Personal Data in accordance with applicable data protection laws.

1. Security Governance & Certifications

The Processor operates an Information Security Management System (ISMS) aligned with:

- **ISO 27001:2022**
- **SOC 2 (Security, Availability, Confidentiality)**

Security controls are reviewed at least annually and enhanced based on emerging threats, audit results, and risk assessments.

2. Cloud Infrastructure & Shared Responsibility

The Processor uses **AWS** as its cloud service provider.

- **AWS** ensures physical security, data center operations, network infrastructure, and virtualization layers.
- **Processor** ensures security of systems, applications, data, IAM, monitoring, logging, encryption, and incident response within the cloud.

Sub-processors undergo security and legal review, and contracts include data protection and confidentiality obligations.

3. Data Encryption & Key Management

- Personal Data is encrypted **in transit (TLS 1.2+)** and **at rest** using industry-standard algorithms (AES-256 or equivalent).
- Encryption keys are managed with AWS KMS, with strict access controls, separation of duties, and periodic audits.
- The Processor retains control over key lifecycle activities (generation, rotation, usage, and revocation).

4. Access Control & Identity Management

- Access follows the **principle of least privilege**.
- Unique IAM accounts for all administrators; **Multi-Factor Authentication (MFA)** is mandatory.
- Role-Based Access Control (RBAC) restricts access to authorized personnel.
- Administrative activities are logged and continuously monitored.

5. System Hardening, Patching & Change Control

- Access follows the **principle of** Standardized secure configuration baselines are enforced across systems and cloud resources.
- Regular patching and vulnerability remediation processes are in place.

- Production changes follow a documented **Change Management** process with approvals and tracking.

6. Monitoring, Logging & Auditing

- Continuous monitoring using **AWS CloudTrail, AWS Config**, and Cloud Security Posture Management (CSPM) tools.
- Security logs are retained and reviewed for suspicious or unauthorized activity.
- Regular internal and external audits validate compliance with security policies and regulatory requirements.

7. Incident Detection & Response

- A documented Incident Response Policy covers detection, investigation, containment, eradication, and recovery.
- The Incident Response Team is trained and operates cross-functionally.
- Any security incident affecting Personal Data is reported to the Controller **without undue delay**, in line with contractual requirements.

8. Data Retention & Secure Deletion

- Personal Data is retained only as long as necessary for contractual or legal requirements.
- Secure deletion uses cryptographic erasure or industry-recognized sanitization methods.
- Evidence of deletion is maintained; deletion confirmations are obtained from third parties where applicable.

9. Business Continuity & Disaster Recovery

- The Processor maintains documented Business Continuity and Disaster Recovery (BC/DR) plans.
- These plans are tested periodically to ensure service resilience, high availability, and data integrity.
- Capacity management and stress testing ensure that systems perform reliably under expected and peak loads.

ANNEX III

LIST OF SUB-PROCESSORS

Seclore engages Sub-Processors who have or potentially will have access to or Process Personal Data on behalf of Seclore.

The below table lists the names and various functions performed by the Sub-Processors:

Sub-processor	Description of Processing	Hosting Location(s)	Applicable Data Protection Terms
Amazon Web Services, Inc.	Cloud infrastructure hosting	U.S.	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Fresh Desk	Support ticketing platform	U.S.	https://www.freshworks.com/legal/
Protecto.io	Data masking services	U.S.	This DPA

Unless otherwise specified above, the nature and duration of each Sub-Processor's activity is the following:

Nature: Assisting Seclore in fulfilment of the purposes of the Agreement.

Duration: The term of Seclore's agreement with the Sub-Processor, unless earlier deletion or return is requested by Seclore. For additional information, please see "Applicable Data Protection Terms" in the table above.

Sub-Processor Security

Seclore assesses the security posture of all Sub-Processors before use and periodically thereafter to validate that the Sub-Processor implements a security program in accordance with Seclore's security policy for the categories of Personal Data Processed by the Sub-Processor. Further, Seclore establishes contractual safeguards with its Sub-Processors through data processing agreements.