DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") sets forth the terms for the processing and protection of Personal Data, in connection with ClientClient's utilization of Beazley Security, LLC's (individually, "Beazley Security", collectively, the "Parties") Services, in compliance with all applicable Data Protection Laws.

By using the Services provided by Beazley Security, the Client agrees to be bound by the terms of this Data Processing Agreement (DPA). This DPA is intended to operate from one or more Statements of Work (SOWs) and forms an integral part of the agreement between the parties.

1. Definitions

- **"Anonymization"** means the irreversible process of transforming Personal Data so that a Data Subject can no longer be identified, directly or indirectly, by any means reasonably likely to be used by any party.

- **"Business"** has the meaning set forth in the California Consumer Privacy Act (CCPA) and refers to the entity that determines the purposes and means of processing Personal Data for commercial purposes.

- **"Consumer"** has the meaning set forth in the CCPA and refers to a natural person who is a California resident, as defined under applicable law.

- **"Controller"** "Data Controller", and "Client" means the entity that determines the purposes and means of the processing of Personal Data and owns the Personal Data, as defined under GDPR. For purposes of this Agreement, "Controller" shall also mean "Business" as defined under the CCPA, to the extent applicable.

- **"Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

- **"Data Protection Laws"** means all applicable and binding privacy and data protection laws and regulations, including but not limited to:
    - The European Union General Data Protection Regulation (GDPR);
    - State-specific laws within the United States including the California Consumer Privacy Act (CCPA)
    - Any other applicable laws or regulations concerning privacy and data protection as updated, amended, or replaced from time to time.

- **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates, as defined under GDPR. For purposes of the CCPA, this term also includes a "Consumer."

- **"Personal Data"** or "Personal Information" means any information that relates to an identified or identifiable natural person, as defined under GDPR, or any information that identifies, relates to, describes, or is reasonably capable of being associated with a particular Consumer, as defined under the CCPA.

- **"Processing"** means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, alteration, retrieval, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.

- **"Processor"** or "Data Processor" is Beazley Security, LLC and is the entity that processes Personal Data on behalf of the Controller, as defined under GDPR. For purposes of the CCPA, this term shall also mean "Service Provider."

- **"Pseudonymization"** means the processing of Personal Data in such a manner that the data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure non-attribution.

- **"Sale"** or **"Selling"** has the meaning set forth in the CCPA and refers to the exchange of Personal Data for monetary or other valuable consideration. This term excludes disclosures for business purposes as defined in the CCPA.

- **"Sensitive Data"** or "Sensitive Personal Information" means Personal Data that requires additional protection under applicable Data Protection Laws, including:
    - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
    - Genetic data, biometric data, or data concerning health, sex life, or sexual orientation;

- Data concerning criminal convictions and offenses; and

- **"Sensitive personal information"** as defined under the CCPA, including Social Security numbers, financial account information, and precise geolocation data.

- **"Standard Contractual Clauses (SCCs)"** means the standard clauses adopted by the European Commission for the transfer of Personal Data to third countries that do not ensure an adequate level of protection under GDPR, including any subsequent amendments or revisions.

- **"Sub-Processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller, as further specified under GDPR Article 28(2).

- **"Supervisory Authority"** means an independent public authority established pursuant to GDPR Article 51 to monitor compliance with GDPR or an equivalent authority under applicable Data Protection Laws.

- **"Technical and Organizational Measures"** means the security measures implemented by the Processor to protect Personal Data, including measures described in Schedule 2, which are appropriate to the risks presented by the processing.

2. Processing of Personal Data

(A) Scope and Purpose of Processing.

(1) The Processor shall process Personal Data solely on behalf of and in accordance with the documented instructions of the Controller, as specified in a Statement of Work (SOW), and Schedule 1 (Details of Processing). Processing shall be limited to the purposes outlined in Schedule 1 unless otherwise agreed in writing.

(2) The Processor shall not process Personal Data for any purpose other than those explicitly set forth in this Agreement or as required by applicable law. If required by law, the Processor shall inform the Controller of such a legal requirement before processing, unless prohibited from doing so by law.

(B) Details of Processing. The subject matter, nature, purpose, duration, types of Personal Data, and categories of Data Subjects involved in the processing are detailed in Schedule 1 (Details of Processing). The specific data elements processed for a given Client shall be as described in an applicable SOW.

(C) Technical and Organizational Measures. The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to protect against unauthorized or unlawful processing and against accidental data loss, destruction, or damage of Personal Data. These measures are compliant with ISO 27001:2022, ISO 27701:2019, and SOC 2 Type 2 compliance frameworks.

(D) Assistance with Compliance. Taking into account the nature of the processing, the Processor shall assist the Controller in ensuring compliance with its obligations under applicable Data Protection Laws by providing relevant privacy and security compliance certifications for ISO 27001:2002, ISO 27701:2019, and SOC 2 Type 2, and the Processor's external Internal Security Controls document and shall be subjected to the Non-Disclosure Clause as stated in the Master Services Agreement (MSA).

(E) Client's Obligation Not to Provide Sensitive Data

(1) The Client shall not knowingly provide, transmit, or otherwise make available to Beazley Security any Sensitive Data (as defined under applicable Data Protection Laws), including but not limited to:

(a) Special Categories of Personal Data under GDPR Article 9 (e.g., health data, biometric data, or data revealing racial or ethnic origin);

(b) Personal Data relating to criminal convictions or offenses under GDPR Article 10;

(c) Sensitive Personal Information as defined under the CCPA/CPRA (e.g., Social Security numbers, financial account details with access credentials, geolocation data, genetic data); and

(d) Any other categories of sensitive or highly regulated data requiring specific handling beyond the scope of this Agreement.

(2) Handling of Inadvertently Received Sensitive Data. If Beazley Security inadvertently receives Sensitive Data, it shall process such data only to the extent necessary to comply with this Agreement or applicable Data Protection Laws. Upon discovery of the inadvertent receipt of Sensitive Data, Beazley Security may, at its sole discretion:

(a) Securely delete such data and notify the Client;

(b) Return the data to the Client upon request; or

(c) Request written confirmation from the Client as to how the Sensitive Data should be handled.

(3) Liability for Unauthorized Submission of Sensitive Data:

(a) Beazley Security shall bear no liability for the receipt, processing, loss, or exposure of Sensitive Data that the Client provides in violation of this section.

(b) The Client agrees to indemnify, defend, and hold harmless Beazley Security from any claims, fines, damages, or regulatory penalties arising from the Client's unauthorized submission of Sensitive Data.

3. Sub-Processors

(A) Engagement of Sub-Processors.

(1) The Client acknowledges and agrees that Beazley Security engages third parties ("Sub-Processors") to support the provision of the Services. Sub-Processors may perform data processing activities on behalf of Beazley Security under this Agreement.

(2) Beazley Security shall ensure that all Sub-Processors are bound by written agreements to obligations no less protective of Personal Data than those set forth in this Agreement and applicable Data Protection Laws.

(B) Sub-Processor List & Updates

(1) Beazley Security maintains a current list of authorized Sub-Processors, including their names, locations, and the nature of their processing activities. This list is available at https://beazley.security/privacy-cookie-policies and incorporated by reference in this Agreement.

(2) The Sub-Processor list shall be updated as necessary to reflect any additions, removals, or changes to Sub-Processors. The Client is responsible for reviewing the list periodically to stay informed of any changes.

(C) Advance Notice of New Sub-Processors. Beazley Security shall notify the Client in writing of any intended changes to the Sub-Processor list, including the addition or replacement of any Sub-Processor, at least thirty (30) days before such changes take effect. Notice may be provided via email, a public posting on the Sub-Processor list webpage, or another reasonable method.

(D) Sub-Processor Objection Process

(1) The Client may object to the engagement of a new Sub-Processor within fifteen (15) days of receiving written notice, but only on reasonable, documented grounds relating to data protection risks. If no objection is received within the 15-day period, a new Sub-Processor shall be deemed accepted.

(2) If the Client raises a valid objection, the Parties shall work together in good faith to address the Client's concerns, which may include:

i. Providing additional safeguards to mitigate the identified risks;

ii. Offering an alternative solution to avoid processing by the proposed Sub-Processor.

(3) If the Parties are unable to resolve the objection within thirty (30) days, the Client may terminate the affected services upon written notice, without liability for such termination, provided that such services cannot reasonably be performed without the proposed Sub-Processor.

(E) Liability for Sub-Processors. Beazley Security shall remain responsible to the Client for the performance of its Sub-Processors' obligations under this Agreement, except where Beazley Security has ensured that the Sub-Processor is contractually bound to equivalent obligations and has taken reasonable steps to verify compliance, in which case the Sub-Processor would bear direct responsibility to Client The Client agrees that Beazley Security shall not be liable for any processing conducted by a Sub-Processor if such processing is performed in accordance with the terms of this Agreement and applicable Data Protection Laws.

(F) Access to Sub-Processor Information. Beazley Security shall provide, upon written request by the Client, relevant details about its Sub-Processors to the extent reasonably necessary to demonstrate compliance with applicable Data Protection Laws. However, Beazley Security shall not be required to disclose information or do so in a manner that would breach written obligations with its Sub-Processors.

4. Data Breach Notification

(A) Notification Obligations.

The Processor shall notify the Client without undue delay, and in any event no later than **48 hours** after becoming aware of a Personal Data Breach affecting the Client's Personal Data, unless prohibited by law. Beazley Security will notify the Client through Beazley Security's Incident Response and Security Team or its Privacy Team, which may be contacted at privacy@beazley.security.com.

(B) Content of Notification. The notification shall include, to the extent reasonably available:

(1) A description of the nature of the breach, including the categories and approximate number of data subjects and records affected;

(2) The likely consequences of the breach;

(3) The measures taken or proposed to address the breach and mitigate its potential effects; and

(4) The name and contact details of the Processor's designated contact point for further information.

(C) Ongoing Updates. The Processor shall provide regular updates to the Client on the status of the investigation, containment, and remediation efforts until the breach is resolved.

(D) Support for Compliance. The Processor shall cooperate fully with the Client to enable the Client to comply with its obligations under applicable Data Protection Laws, including:

(1) Providing additional information reasonably requested by the Client;
(2) Assisting in the preparation of any required notifications to Supervisory Authorities or data subjects; and
(3) Taking steps to mitigate the effects of the breach and prevent future occurrences.

(E) Notification to Third Parties. The Processor shall not disclose details of a Personal Data Breach to any third party without the Client's prior written consent, except:

(a) where required by applicable law, regulation, or a binding order of a Supervisory Authority; or
(b) where disclosure is necessary to third parties acting as agents of the Processor in support of breach investigation, mitigation, remediation, or legal compliance efforts (e.g., IT security personnel, forensic investigators, external legal counsel).The Processor shall ensure that any such third parties are bound by confidentiality and security obligations no less protective than those set forth in this Agreement.

5. Data Subject Rights

(A) Assistance with Data Subject Requests

(1) The Processor shall assist the Client in responding to Data Subject requests to exercise their rights under applicable Data Protection Laws, including but not limited to:

(a) **Access**: The right to obtain confirmation of whether Personal Data is being processed and access to such data (GDPR Article 15; CCPA §1798.100).
(b) **Rectification**: The right to correct inaccurate or incomplete Personal Data (GDPR Article 16).
(c) **Erasure ("Right to Be Forgotten")**: The right to request the deletion of Personal Data, subject to applicable exceptions (GDPR Article 17; CCPA §1798.105).
(d) **Restriction of Processing**: The right to restrict the processing of Personal Data in specific circumstances (GDPR Article 18).
(e) **Data Portability**: The right to receive Personal Data in a structured, commonly used, and machine-readable format and to transmit it to another controller (GDPR Article 20).
(f) **Objection to Processing**: The right to object to the processing of Personal Data, including for direct marketing purposes (GDPR Article 21; CCPA §1798.120).
(g) **Do Not Sell or Share**: For California residents, the right to opt out of the sale or sharing of Personal Data (CCPA §1798.120).

(2) The Client shall notify Beazley Security of any data subject rights request by submitting them by email to privacy@beazley.security.com.

(B) Controller Instructions

(1) The Processor shall not respond to any Data Subject request directly unless explicitly instructed to do so by the Controller or required by law.

(2) Where required by law, the Processor shall:
(a) Inform the Controller of the legal requirement before responding, unless prohibited by law; and
(b) Limit the response to the minimum scope necessary to comply with the legal obligation.

(C) Costs of Compliance. The Processor shall not charge for assistance with Data Subject requests unless:

(1) The requests are manifestly excessive, repetitive, or unfounded, in which case the Processor may charge a reasonable fee or refuse to act on the request, subject to applicable law; or
(2) Such costs are agreed upon in writing in advance.

(D) Record-Keeping and Reporting

(1) The Processor shall maintain a log of all Data Subject requests received and processed, including:
(a) The type of request (e.g., access, rectification, deletion);
(b) The date the request was received and forwarded to the Controller;
(c) Actions taken to comply with the request; and
(d) The date of final resolution.

(2) The Processor shall provide this log to the Controller upon request to demonstrate compliance with applicable Data Protection Laws.

(3) Client may request an adjusted timeline of Personal Data retention provided such request is technically feasible, commercially reasonable and the Client is responsible for any associated costs.

(E) Handling of Do Not Sell or Share Requests. The Processor shall assist the Controller in complying with Do Not Sell or Share requests under the CCPA, or analogous legal mechanism, by:

(1) Ensuring Personal Data is not disclosed in exchange for monetary or other valuable consideration;
(2) Implementing technical measures to restrict the sharing of Personal Data unless explicitly authorized by the Controller; and
(3) Providing confirmation to the Controller that such requests have been honored.

6. Data Audits

(A) Annual Audits. Processor may provide certifications, such as ISO 27001 or SOC 2 Type II reports, as evidence of compliance in lieu of on-site audits, subject to the Client's review and acceptance. If the Client does not accept such certifications, the Client may conduct one (1) audit per calendar year of the Processor's compliance with this Agreement and applicable Data Protection Laws, subject to the following conditions:

(1) The Client shall provide at least **thirty (30) days' prior written notice** of its intent to conduct an audit.
(2) The audit shall be conducted during the Processor's normal business hours and in a manner that minimizes disruption to the Processor's operations.
(3) Following a confirmed or suspected Personal Data Breach involving the Processor, an ad-hoc audit may be requested by the Client at Client's expense.

(B) Scope of Audits. The audit shall be limited to the Processor's systems, processes, and facilities that are directly involved in processing the Client's Personal Data. The Client may not access or audit unrelated systems or information.

(C) Third-Party Auditors.

(1) The Client may appoint an independent third-party auditor to conduct the audit, provided the auditor is subject to confidentiality obligations equivalent to those in this Agreement and is not a direct competitor of Beazley SEc.
(2) The Processor may object to the Client's choice of auditor on reasonable grounds, including conflict of interest, and propose an alternative.

(D) Costs of Audits.

(1) The Client shall bear its own costs in connection with audits, except that the Processor shall reimburse the reasonable costs of an audit if the audit reveals material non-compliance with this Agreement or applicable Data Protection Laws that results in a material risk to the security or privacy of Personal Data.
(a) For the purposes of Sub-Section (E)(1)), "material non-compliance" shall not include: minor administrative or technical errors that do not meaningfully impact data protection; findings that do not require corrective action under applicable Data Protection Laws; or compliance gaps that do not create a material risk of unauthorized disclosure, loss, or corruption of Personal Data.
(b) Where an audit reveals only immaterial or technical compliance issues, the Client shall bear the full cost of the audit.

(E) Use of Audit Findings. The Parties shall discuss the findings of any audit and agree on an action plan to address any identified non-compliance. The Processor shall implement reasonable corrective actions within an agreed timeframe or else within ninety (90) days. If Beazley Security determines, in its reasonable discretion, that any requested remediation is commercially unreasonable, it shall notify the Client in writing, providing a rationale for its decision.

7. Cross-Border Data Transfers

(A) General Principles. The Client acknowledges and agrees that Beazley Security operates on a global infrastructure and provides its services through international data centers, personnel, and Sub-Processors. As a result, Personal Data processed under this Agreement will be transferred across borders, including to jurisdictions that may not provide the same level of data protection as the Client's country of origin. This Agreement is intended for Clients who have agreed to receive services from Beazley Security on a global basis, with cross-border data transfers as an inherent part of service delivery. If a Client requires specific restrictions on cross-border transfers, such restrictions shall only apply if agreed upon in a separate written agreement executed by both Parties. Such transfers may occur between jurisdictions, including but not limited to the EEA, UK, U.S., Canada, Australia and Singapore.

(B) Mechanisms for Transfers. If Beazley Security transfers Personal Data outside of the EEA, UK, or other jurisdictions with similar data protection laws, such transfers will be conducted in compliance with applicable Data Protection Laws using an approved transfer mechanism (e.g., adequacy decision, Standard Contractual Clauses, or another legally recognized framework).

(C) Transfer Impact Assessments (TIAs). For transfers subject to SCCs or equivalent mechanisms and only where additionally required by applicable data protection laws, Beazley Security shall conduct and document a Transfer Impact Assessment (TIA) to

assess the legal framework of the destination country and the likelihood of interference with the transferred Personal Data. Beazley Security shall implement supplementary measures where necessary to address identified risks.

(D) Sub-Processor Obligations. Beazley Security shall ensure that all Sub-Processors engaged for cross-border transfers comply with the mechanisms and safeguards outlined in this section. Sub-Processors shall execute SCCs or equivalent agreements and implement supplementary measures, where required. Beazley Security shall provide the Client with evidence of Sub-Processor compliance upon request.

8. Return or Deletion of Personal Data

(A) Retention by the Processor. Personal Data shall be retained only for as long as necessary to fulfill the purposes of processing as outlined in an applicable SOW, Schedule 1 or to comply with legal obligations. Beazley Security shall ensure that all Sub-Processors engaged under Section 3 are obligated to analogous return and deletion policies or that such policies otherwise comply with applicable Data Protection Laws.

(B) Deletion or Return of Data. Upon termination of this Agreement or at the Client's written request, the Processor shall:

(1) Return all Personal Data to the Client in a commonly used, machine-readable format; or

(2) Permanently delete all Personal Data, including copies, from its systems and those of its Sub-Processors, unless retention is required by applicable law or other measures are specified in an applicable Statement of Work (SoW).

(C) Handling of Backup Data

(1) For Personal Data stored securely within backup systems that cannot be immediately deleted for technical reasons, the Processor shall:

i. Flag the data as "restricted," ensuring it is not accessible for any active processing purposes;

ii. Mark the data for destruction within the standard backup retention schedule; and

iii. Permanently delete the data when the backup media is overwritten or securely disposed of in the ordinary course of backup maintenance.

(2) Personal Data retained in backup systems under subsection (a) shall be considered deleted once it is flagged for destruction and segregated from active processing environments, provided the Processor ensures its eventual secure destruction.

(D) Confirmation of Deletion. The Processor shall provide written confirmation to the Client, upon written request, that all Personal Data, including backup data subject to subsection 3, has been flagged for destruction or deleted in accordance with this section.

9. Liability and Indemnification

(A) Liability Cap. Except as provided in Section 9(B) (Exceptions to Liability Cap), each Party's total aggregate liability under this Agreement, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid or payable by the Client under the applicable SOW in the twelve (12) months preceding the event giving rise to liability.

(B) Exceptions to Liability Cap. The liability cap set forth in Section 9(A) shall not apply to:

(1) A Party's indemnification obligations under Section 9(D) (Indemnification);

(2) A Party's gross negligence, willful misconduct, or fraud;

(3) Breach of confidentiality obligations under this Agreement;

(4) Failure to comply with Section 3 (Sub-Processors), except that the Client's liability under Section 3 shall also be capped in accordance with Section 9(A);

(5) Regulatory fines or penalties imposed directly on a Party by a Supervisory Authority or other government agency for non-compliance with applicable Data Protection Laws, to the extent such fines are not the result of the other Party's breach.

(C) Exclusion of Indirect Damages. Neither Party shall be liable for indirect, incidental, consequential, punitive, or special damages, including but not limited to loss of profits, revenue, business opportunities, goodwill, or anticipated savings, arising out of or related to this Agreement, even if the Party has been advised of the possibility of such damages. This exclusion shall not apply to liabilities that fall under Section 9(B) (Exceptions to Liability Cap).

(D) Indemnification

(1) Beazley Security's Indemnification Obligations. Beazley Security shall indemnify, defend, and hold harmless the Client from and against any third-party claims, damages, liabilities, fines, or penalties, including reasonable attorney's fees, to the extent arising from:

(a) Beazley Security's material breach of this Agreement or applicable Data Protection Laws;

(b) Unauthorized Processing or disclosure of Personal Data caused by Beazley Security's failure to implement required security measures;

(c) Breach of confidentiality obligations under this Agreement.

(2) Client's Indemnification Obligations. The Client shall indemnify, defend, and hold harmless Beazley Security from and against any third-party claims, damages, liabilities, fines, or penalties, including reasonable attorney's fees, to the extent arising from:

(a) The Client's failure to comply with Section 3 (Sub-Processors), except that the Client's liability shall remain subject to Section 9(A) (Liability Cap);

(b) Any regulatory fines or penalties imposed on Beazley Security due to the Client's instructions or actions in violation of applicable Data Protection Laws;

(c) The Client's intentional misuse or unauthorized sharing of Beazley Security's services or infrastructure leading to a security incident.

(3) Indemnification Process. A Party seeking indemnification shall:

(a) Provide prompt written notice of the claim;

(b) Allow the indemnifying Party sole control over the defense and settlement of the claim, provided that any settlement does not impose liability or obligations on the indemnified Party beyond monetary damages; and

(c) Cooperate in good faith in the defense of such claim.

(E) Allocation of Regulatory Fines and Penalties

(1) Each Party shall bear responsibility for regulatory fines or penalties imposed directly on it due to its own non-compliance with applicable Data Protection Laws.

(2) If a fine is imposed on Beazley Security due to the Client's non-compliance or processing instructions, the Client shall indemnify Beazley Security for the portion of the fine attributable to its actions.

(3) This provision shall not be interpreted to limit or exclude any statutory rights or remedies available to Data Subjects under GDPR Article 82 or similar laws.

10. Governing Law and Jurisdiction

This Agreement is governed by and construed in accordance with the laws of the Commonwealth of Massachusetts, and any disputes arising under this Agreement shall be subject to the exclusive jurisdiction of the state and federal courts of Massachusetts.

11. Survival

The obligations set out in this Agreement shall survive the termination or expiration of any applicable parent agreement for as long as the Processor retains Personal Data or the Parties remain actively engaged with respect to the continued provision of Services by Beazley Security to the Client but have yet to enter into a later SOW or other binding contract.

12. Miscellaneous

(A) Severability. If any provision of this Agreement is deemed invalid or unenforceable, the remainder shall continue in effect.

(B) Modifications. Beazley Security reserves the right to update this DPA from time to time to reflect changes in applicable laws or service practices. Such updates shall not materially degrade the service or the processing of data. Clients are encouraged to review the DPA regularly to stay informed of any modifications.

SCHEDULE 1 – DETAILS OF DATA PROCESSING

1. Subject Matter of Processing
The processing of Personal Data is undertaken to enable the Processor to provide the services described in any applicable and this Agreement. Processing activities include collecting, storing, analyzing, transmitting, and deleting Personal Data as instructed by the Controller.

2. Nature and Purpose of Processing
The Processor shall process Personal Data to provide services agreed upon in the Statement of Work (SoW).
The processing activities include, but are not limited to:

- Collecting Personal Data to enable the provision of services;
- Analyzing data for operational or security purposes;
- Storing Personal Data in a secure environment;
- Transmitting Personal Data as required for service delivery; and
- Deleting or returning Personal Data upon completion of services or termination of the Agreement.

3. Duration of Processing
The Processor shall process Personal Data for the duration of an applicable SOW, unless:

- Otherwise instructed in writing by the Controller; or
- Retention is required by applicable laws or regulations.

Upon termination of the Agreement, the Processor shall delete or return all Personal Data, including any copies held by Sub-Processors, as specified in Section 8 of this Agreement.

4. Categories of Data Subjects
Personal Data processed by the Processor may relate to the following categories of Data Subjects:

- Employees, contractors, and representatives of the Controller;
- End users of the Controller's systems or services;
- Clients, suppliers, and business contacts of the Controller;
- Other individuals whose data is provided by the Controller in accordance with the Agreement.

5. Types of Personal Data
The Processor may process the following types of Personal Data, as determined by the Controller:

- **Identification Data**: Name, email address, phone number, job title, department;
- **IT Data**: IP addresses, device IDs, MAC addresses, session logs, login credentials (encrypted);
- **Professional Data**: Employer name, system usage logs, access history, Email transaction logs, including subject lines, sender/recipient data, and attachment metadata;
- **Transactional Data**: Invoices, billing records, and other contractual details;
- **Other Data**: Any additional categories of Personal Data explicitly provided by the Controller.

6. Processing of Sensitive Data
Sensitive Data is not anticipated to be processed under this Agreement as Client is under an obligation not to provide such data. The handling of Sensitive Data received notwithstanding to this obligation is addressed by Section 2(H).
The following types of data constitute Sensitive Data unless special conditions apply:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for identification purposes
- Health data
- Data concerning a person's sex life or sexual orientation

7. Frequency of Processing
Personal Data shall be processed on a continuous or recurring basis throughout the duration of the Agreement unless specified otherwise by the Controller.

8. Retention and Deletion of Personal Data

- **Retention by the Processor**: Personal Data shall be retained only as necessary to fulfill the purposes of processing or comply with legal obligations. The Processor shall not retain Personal Data longer than instructed by the Controller.
- **Retention by Sub-Processors**: The Processor shall ensure that all Sub-Processors adhere to equivalent retention and deletion requirements.
- **Deletion or Return**: Upon termination of the Agreement, the Processor shall securely delete or return Personal Data to the Controller and confirm such deletion or return in writing.

Archived or backup data containing Personal Data shall also be securely deleted within 30 days, unless otherwise required by law.

9. Sub-Processor Processing

For transfers of Personal Data to Sub-Processors, the following shall apply:

- Sub-Processors shall process Personal Data solely for the subject matter, nature, and duration required to provide services specified in an applicable SOW;
- Sub-Processors shall comply with the obligations outlined in this Agreement, including retention and deletion requirements; and
- The Processor shall provide the Controller with a list of Sub-Processors and their processing activities upon request.

10. Regular Updates to Schedule

The Controller and Processor shall review and update this Schedule annually or as necessary to reflect changes in processing activities, categories of Personal Data, or Data Subjects. The Processor shall notify the Controller of any material changes that may affect this Schedule.