I. DEFINITIONS:

Unless otherwise stated or unless the context otherwise requires, each capitalized term will have the meaning set out below. Terms used but not otherwise defined in this Section shall have the meanings ascribed to them in the Data Protection Laws.

a) **Data Controller-** shall mean an entity that determines the purposes and means of the Processing of Personal Data. For avoidance of doubt, the parties agree and acknowledge that "Data Controller" is being used for convenience only. Therefore, all equivalent terms defined in the applicable Data Protection Laws shall be deemed to be referred as Data Controller for the purposes of this DPA, such but not limited to, "business" under CCPA or "organisation" under SPDPA.

b) **Data Protection Laws -** shall mean all applicable data protection and privacy laws applicable to the Personal Data Processed by the Processor, including without limitation to, the EU General Data Protection Regulation (2016/679) ("**GDPR**"), the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction ("**ePrivacy Directive**"), GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2018, the California Consumer Privacy Act, 2018 ("**CCPA**") the Singapore Personal Data Protection Act 2012 ("**SPDPA**") as amended, replaced or equivalent legislation applicable to the Services from time to time and all legislation protecting the fundamental rights and freedom of persons and their rights to privacy and security of information applicable to the Processing of Personal Data;

c) **Data Processor-** shall mean an entity that Processes Personal Data on behalf of the Data Controller. For avoidance of doubt, the parties agree and acknowledge that "Data Processor" is being used for convenience only. Therefore, all equivalent terms defined in the applicable Data Protection Laws shall be deemed to be referred as Data Processor for the purposes of this DPA, such but not limited to, "service provider" under CCPA or "data intermediary" under SPDPA.

d) **Data Subject-** means the identified or identifiable natural person to whom the Personal Data shared with the Processor under this DPA relates. For avoidance of doubt, the parties agree and acknowledge that "Data Subject" is being used for convenience only. Therefore, all equivalent terms defined in the applicable Data Protection Laws shall be deemed to be referred as Data Subject for the purposes of this DPA, such but not limited to, "consumer" under CCPA or "individual" under SPDPA.

e) **Personal Data-** shall mean any information, including opinions, relating to an identified or identifiable natural person (and includes similarly defined terms under the applicable Data Protection Laws) Processed under this DPA for the purposes of the Agreement, including without limitation, Personal information, sensitive personal information, special categories of personal data, derived personal data, as defined respectively under the applicable Data Protection Laws for the purposes of the Services.

f) **Process-** shall mean any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collecting, gathering, obtaining, receiving, accessing, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, aligning or combining, restricting, erasing, destroying, using, disclosing by transmission, dissemination, or otherwise making available and the terms "**Processing**", "**Processed**" and "**Processes**" shall be construed accordingly.

g) **Standard Contractual Clauses-** shall mean the contractual clauses set out in the European Commission's Decision of 4th June 2021 on standard contractual clauses for the transfer of Personal Data to Processors established in third countries, under the Data Protection Laws, as may be amended by the European Commission from time to time; and

h) **Security Incident-** shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data

i) **Special Categories of Personal Data -** shall mean and include any categories of Personal Data that have been accorded a special status under the applicable Data Protection Laws

due to their nature and need a higher standard of care when being handled, including without limitation, medical or health information, racial or ethical origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, sex life and sexual orientation.

j) **Sub-processor-** shall mean any downstream processors used by the Data Processor to Process Personal Data while providing the Services to the Data Controller.

k) **Supervisory Authority-** shall mean the relevant supervisory or regulatory authority with responsibility for privacy or data protection matters in the jurisdiction of the Data Controller.

II. ROLE AND SCOPE OF PROCESSING:

1. **Role**. As between the parties, Atlan (as defined in the Agreement) and all its Affiliates that may Process Personal Data under this DPA shall be deemed as the "Data Processor" (or Sub-processor, as applicable) acting on behalf of the Customer. The parties agree that Customer Affiliates (as defined in the Agreement) may request for Services under this Agreement and as such, for the purposes of this DPA, in the event, the Customer Affiliates require Processing of Personal Data: (a) the Customer must confirm the instructions provided by its Affiliates and their Users; (b) the Customer shall ensure that the terms of this DPA are appropriately flowed down to its Affiliates and shall remain liable to the Data Processor for any non-compliance by its Affiliates of this DPA; and (c) any claims against the Data Processor related to this DPA shall be exclusively brought by the Customer and shall be subject to any liability restrictions set forth in the Agreement, including, but not limited to, any aggregate limitation of liability.

2. **Scope of Processing**

a. Purposes. Processing of Personal Data under this DPA shall be solely limited to the provision of Services and only as instructed by the Data Controller, including without limitation, any support services provided by the Data Processor for which it may need to access Personal Data. For clarity, if the Data Processor doubts the legality of the instructions provided by the Customer, it has the right to clarify its doubts prior to Processing the Personal Data and shall not be liable for any claims or non-compliance with Data Protection Laws if it acts on the instructions of the Customer. Furthermore, in the event any instructions provided by the Data Controller are held to be illegal and/or non-compliant with the applicable Data Protection Laws and the Data Processor is held liable for the same, the Customer shall indemnify the Data Processor under Section 10b. of the Agreement.

b. Prohibitions on Processing. Data Processor agrees that it is prohibited from:

(i) selling any Personal Data received under this DPA; and/or
(ii) acting contrary to the Data Controller's instructions except where it doubts the legality of the instructions whereunder it may delay Processing until its doubts are clarified by the Data Controller; and/or
(iii) using or in any way Processing the Personal Data received hereunder for any purposes other than to deliver Services to Data Controller or otherwise without Data Controller's express written consent; and/or
(iv) retaining, using, or disclosing the Personal Data (i) for any purposes (including commercial purposes) other than for provision of Services or (ii) outside the direct business relationship between the parties unless, in each case, expressly permitted by the applicable Data Protection Laws.

c. Notice of inability to comply with obligations under this DPA. Atlan shall promptly notify the Customer, in writing, if it determines that it can no longer meet its obligations under this DPA. Upon such notice, Customer may direct the Data Processor to take

reasonable and appropriate steps to remediate the inability and may ask for temporary suspension of Processing.

d. Categories of Data Subjects and Personal Data Processed. The categories of Data Subjects to whom the Personal Data relates and categories of their Personal Data (including without limitation, contact details, financial information and where applicable special categories or sensitive Personal Data) to be Processed by Atlan under the Agreement shall be solely determined and controlled by the Customer (including where Atlan may be a sub-processor).

e. Retention of Personal Data. Any Personal Data Processed pursuant to the Agreement shall be retained until required for the provision of Services. For avoidance of doubt, any Personal Data retained by the Processor as part of its internal policies and procedures, including any back-up protocols, shall be deleted as per its policies in the ordinary course of business.

III. SUB-PROCESSORS:

1. **Authority to use Sub-processors**. To the extent necessary to fulfil the Services, the Data Controller understands and hereby authorizes the engagement of Sub-processors by the Data Processer to deliver the Services. The list of Data Processor's current Sub-processors is provided at https://security.atlan.com/subprocessors.

2. **Liability for Sub-processors**. The Data Processor shall: (a) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than agreed in this DPA to the extent applicable to the Services provided by the Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA. Upon written request, and subject to any confidentiality restrictions, Data Processer shall provide Customer all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy Customer's obligations under Data Protection Laws.

3. **Changes to Sub-processors**. Any changes to the Sub-processors shall be notified to the Customer as soon as reasonably possible. The Customer may raise an objection to the changed Sub-processor within 15 (fifteen) days from the date of notification by the Data Processor after which it shall be deemed that the Customer has no objections to the new Sub-processor. The objections must be submitted in writing demonstrating reasonable grounds which shall be discussed by the parties in good faith to find a resolution. In the event, the parties are unable to find a resolution within a reasonable time, including without limitation, the Data Processor being unable to provide an alternate Sub-processor, the Customer's sole remedy shall be to terminate the impacted Order Forms.

IV. DATA PROTECTION WARRANTIES AND OBLIGATIONS:

1. Each party agrees and warrants that it shall comply with the applicable Data Protection Laws. Accordingly, the Customer hereby confirms that it has the necessary approvals, permits, licenses, consents from Data Subjects, Data Controllers and/or competent authorities in respect of the instructions provided to the Data Processor under the Agreement, including without limitation, permission for international data transfers by the Data Processor as applicable.

2. The Data Processor warrants and undertakes that while Processing the Personal Data, it shall:

a. not transfer Personal Data outside the Hosting Regions except in accordance with Section VI of this DPA;

b. restrict access to Personal Data only to persons for whom access to such data is necessary for the performance of the Services which shall always be subject to Customer consent;

c. flow down the obligations of confidentiality under Section 7(Confidentiality) of th Agreement and those described under this DPA to all persons authorized to access Personal Data via appropriate written agreements;

d. implement commercially reasonable technical and organizational measures (as further described in **Schedule 2**) to protect any Personal Data Processed by it under the Agreement, including without limitation, Article 32(1) of GDPR and/or SPDPA. For avoidance of doubt, Data Processor retains the right to update the measures described in Schedule 2 from time to time provided that any such updates shall not materially diminish the overall security of the Service or Customer Personal Data;

e. inform the Customer promptly, and in any event within three (3) business days, of any enquiry or complaint received from a Data Subject or Supervisory Authority relating to a Data Subject's rights under the applicable Data Protection Laws; and

f. immediately inform the Customer of any doubts as to the legality of the instructions issued by the Customer and/or its Users.

3. If a law enforcement agency sends Atlan a request to access any Customer Personal Data, Atlan will attempt to redirect the law enforcement agency to request such data directly from the Customer. As part of this effort, Atlan may provide Customer's contact information to the law enforcement agency. If compelled to disclose such data under a written order, then Atlan will give Customer reasonable written notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Atlan is legally permitted to do so.

V. COOPERATION:

1. **Data Subject requests.** In the event Atlan receives any request from Data Subjects or applicable Supervisory Authorities, that relates to a Data Subject's Personal Data, Atlan shall notify the Customer in writing within 72 hours of such request being made and not respond to such communication without Customer's prior written authorization other than to inform the requestor that Atlan is not authorized to directly respond to the request. Atlan shall use commercially reasonably efforts to redirect the request directly to the Customer unless legally prohibited from doing so.

2. **Data Protection Impact Assessments**. Taking into account the nature of the Processing and information available to Atlan, Atlan shall provide any and all information regarding the Services requested by Customer to enable Customer to carry out data protection impact assessments or similar evaluations and assessments where required under the Data Protection Laws, including in relation to its sub-processors.

VI. SECURITY INCIDENT:

The Data Processor shall, as soon as practically possible but no later than 72 hours from the occurrence of a Security Incident, notify to the Customer by e-mail and take reasonable steps to contain, investigate, and mitigate the Security Incident. The Data Processor shall endeavour to provide the Data Controller of any such information that the Data Controller may reasonably request for pertaining to the Security Incident. Customer shall have sole discretion as to whether any notifications will be made following a Security Incident involving Customer Personal Data. Atlan shall cooperate with Customer's efforts to notify affected or potentially affected Data Subjects, regulatory authorities, and/or third parties as required by applicable Data Protection Laws.

VII. INTERNATIONAL DATA TRANSFERS

1. **Hosting Region**. Data Processor will only host Customer Personal Data in the region(s) offered by the Data Processer and selected or configured by the Customer via the Software (the "**Hosting Region**"). Customer is solely responsible for the regions from which its Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its Users and for any subsequent designation of other Hosting Regions. Once Customer has selected a Hosting Region, subject to Sections IV 2 b., c. and d. below, the Data Processor will not Process Customer Personal Data from outside the Hosting Region except as reasonably necessary to provide the Services and to deliver the Purposes envisaged by this DPA, or as necessary to comply with the applicable laws or binding order of a governmental body.

2. **Singapore Personal Data Transfers.** In cases where SPDPA applies, to the extent that the Services involve a transfer of Customer Personal Data by the Data Processor outside of Singapore, the Customer authorizes the Data Processor to transfer the Customer Personal Data across international borders only as necessary and required for the provision of Services. The Data Processor shall notify the Customer, describing the details of transfers of Personal Data outside of Singapore, before any such transfer is made.

3. **European Personal Data Transfers.** In cases where GDPR applies, transfer of Customer Personal Data outside the European Union, European Economic Area or any other jurisdiction to which GDPR applies and always subject to the national laws of the member states which are deemed to be incorporated into this DPA by reference. Schedule 3 attached herewith details the particulars of such transfer.

4. **UK Personal Data Transfers.** In cases where UK GDPR applies, any international data transfers shall remain subject to the terms of the UK GDPR and such transfers shall be governed by the International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018 which is deemed to be incorporated into this DPA by reference. Schedule 3 attached herewith details the particulars of such transfer.

VIII. RETURN AND/OR DELETION OF PERSONAL DATA

Upon expiry or termination of the Agreement or the last Order Form executed by the parties, whichever is later and subject to applicable Data Protection Laws, the Data Processor shall return, or delete as requested by the Customer any time during the Term of the Agreement, the Personal Data in its possession within 30 days from the expiry, termination, or request for deletion. For the purposes of this DPA, deletion would include physical or logical deletion, ensuring that the Personal Data cannot be restored extending to all copies held by the Data Processor, including backups. Logical deletion methods will be considered appropriate if they are multi-pass overwrite methods. The Data Processor will provide written confirmation that deletion has been completed, including the physical deletion and method used. For avoidance of doubt, if any Customer Personal Data is retained in the Data Processor's archives or IT back-up, the Data Processor shall continue to be bound by the Data Protection Laws in relation to the retained Personal Data and delete the same in due course of business as per its internal policies.

IX. DURATION AND TERMINATION:

The term of this DPA shall commence on the Effective Date of the Agreement and conclude concurrent to the Term of the Agreement or the last Order Form executed by the parties, whichever is later. For clarity, in case the parties sign an evaluation agreement prior to signing the Agreement and it requires the signing of this DPA, then the terms agreed under the evaluation agreement shall continue to apply for the entire duration of the parties' business relationship and shall apply to any

and all processing of Personal Data under the Agreement. However, in the case of an unsuccessful evaluation, the DPA shall co-terminate with the expiry or termination of the applicable evaluation agreement.

X. AUDIT

The Data Processor will allow and shall cooperate with the Customer during an audit of the Processing of the Personal Data, on request and at Customer's cost limited to once annually. Audits may be conducted by the Customer and/or its representative after providing a reasonable prior notice of at least 15 days with a request for information. The Customer hereby agrees that in exercising its audit rights under this Section, it shall ensure no harm is caused to the Data Processor's systems or its ability to deliver Services to its customers and the scope of such audit shall extend only to matters concerning Data Processor's compliance with this DPA.

XI. RELATIONSHIP WITH AGREEMENT

1. Parties agree and acknowledge that this DPA replaces and supersedes any existing data processing addendums, attachments, exhibits or standard contractual clauses that the parties may have entered into previously in connection with the Services.

2. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA, if there is any conflict between this DPA and a business associate agreement between Customer and the Data Processor, then the business associate agreement shall prevail.

3. Notwithstanding anything to the contrary in the Agreement or this DPA, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA in connection with the Agreement shall remain subject to any aggregate limitations on liability set out in the Agreement.

XII. Without prejudice to the rights of the Data Subjects, this DPA shall not benefit or create any right or cause of action on behalf of a third party (including a third-party Data Controller).

XIII. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

SCHEDULE 1 – TECHNICAL AND ORGANISATIONAL MEASURES FOR DATA PROTECTION AND SECURITY OF THE DATA

We currently observe the Security Measures described in this Schedule 2. All capitalized terms not otherwise defined herein will have the meanings as set forth in the Agreement. For more information on these security measures, including our SOC 2 Type II/SOC 3 Report, ISO 27001:2022, ISO 27701:2019, ISO/IEC 42001 certificates, HIPAA Report, and Penetration Test Summaries, please visit Atlan's Trust Center at https://security.atlan.com or contact security@atlan.com.

Measures of pseudonymization, encryption of personal data and the protection of data during transmission and storage

In-transit: We enforce TLS 1.2 or higher on all communications with the Atlan platform, including login interfaces and every customer site hosted on the Atlan product(s). Our implementation uses industry-standard algorithms and certificates, with automated certificate management and renewal.

At-rest: All data at rest is encrypted using AES-256 encryption via cloud provider Key Management Service (KMS) with managed key rotation. User passwords are hashed using industry-standard one-way hashing algorithms with salting. Encryption at rest applies to all databases, object storage, backups, and log archives.

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

Atlan has personnel responsible for oversight of security. It has a dedicated security team to implement, investigate and review security controls and incidents.

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

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

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

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. Penetration tests are performed against the application layers and network layers of the Atlan technology stack.

Responsible disclosure: A responsible disclosure program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. We implement a responsible disclosure program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

Measures for user identification and authorization

Authentication: Authentication: Single sign-on integration via SAML 2.0 or OIDC with customer identity providers is supported, enabling the enforcement of multi-factor authentication. For native credential management, strong password policies meeting industry benchmarks are mandated alongside salted cryptographic hashing for storage. Access to platform instances requires prior identity validation, with active sessions governed by automated timeout configurations.

Authorization: Customer Data is stored in storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in our product is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

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

We host our product infrastructure with outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Measures for ensuring events logging

We maintain audit logs that capture information about system behavior, traffic received, system authentication events, and other application requests. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Measures for ensuring system configuration, including default configuration

We harden our server infrastructure using a hardening standard based on a common industry standard.

Measures for internal IT and IT security governance and management

Access review: Access to critical infrastructure is reviewed by our IT team on a quarterly cadence.

Security awareness and training: Internal security training and a compulsory review of our security policies is conducted for all of our employees on onboarding and thereafter, on an annual basis. Phishing simulations are conducted on a regular basis to ensure that our employees are aware of the dangers and how to handle such scenarios.

Measures for certification/assurance of processes and products

We engage independent external auditors to perform audits and provide attestations for the following frameworks: SOC 2 Type II (all 5 Trust Services Criteria), SOC 3, ISO 27001:2022 (Information Security Management), ISO 27701:2019 (Privacy Information Management), ISO/IEC 42001 (AI Management System), HIPAA, and GDPR. Annual penetration testing (network and application) is conducted by independent third-party firms, with remediation verified through retesting.

Measures for ensuring data minimization

Atlan processes and persists metadata on data assets (e.g., schema information, descriptions, lineage, tags, and governance attributes). For features such as Preview and Query, raw data is retrieved in real time from the Customer's connected data sources and displayed to authorized end users; this data is not persisted in the Atlan platform beyond the duration of the session. The Customer retains full control over which data sources are connected, what data the Atlan application has access to, and the permissions governing that access..

Measures for ensuring data quality

We allow users to update the information in their accounts themselves or via requests to its customer support function, the Customer Success Team.

Measures for ensuring limited data retention

We maintain a Data Retention Policy setting out the retention periods for various types of data based on legal requirements, justified interests and the purposes of collection.

Measures for ensuring accountability

We have appointed a Data Protection Officer.

Measures for allowing data portability and ensuring erasure

We have a process in place to ensure that our users are able to exercise their rights to data portability and erasure as described in our Privacy Notice available at https://atlan.com/privacy-policy/?ref=/.

Measures for responsible AI governance

Atlan maintains an AI Management System certified under ISO/IEC 42001, covering AI risk assessment, impact analysis, lifecycle management, and governance. AI systems are classified by risk level, with documented controls for transparency, fairness, and human oversight. An AI Governance Committee provides executive oversight of AI-related risks and decision-making. AI policies are reviewed and updated on a regular cadence, with employee training and policy acknowledgment tracked for compliance.

Measures for sub-processor and third-party risk management

Atlan maintains a third-party risk management program to assess the security posture of sub-processors and critical vendors. Assessments include review of SOC 2 reports, ISO certifications, penetration test summaries, data processing agreements, and security questionnaires. All vendors are subject to annual reassessment. An up-to-date list of sub-processors is maintained on https://security.atlan.com/ and made available to customers in accordance with the DPA.

SCHEDULE 2: DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred	Users accessing the Services
Categories of personal data transferred	User credentials, unless otherwise agreed mutually by the parties
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	Not applicable unless included or embedded in the Customer Data
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continuous as required for the provision of Services
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Until the expiry or termination of the Agreement and disengagement of Services.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Continuous as required for the provision of Services