ATLAN DATA PROTECTION ADDENDUM

BY INDICATING YOUR ACCEPTANCE OF ATLAN'S SOFTWARE AS A SERVICE AGREEMENT ("**AGREEMENT**") OR ACCESSING OR USING ANY ATLAN OFFERINGS, IF YOU ARE PROCESSING PERSONAL DATA (AS DEFINED HEREIN) YOU ARE ACCEPTING THE TERMS OF THIS DATA PROCESSING ADDENDUM ("**DPA**") AND THIS DPA SHALL BE BINDING ON BOTH PARTIES TO THE ORDER FORM (AS DEFINED IN THE AGREEMENT). PLEASE READ THESE TERMS CAREFULLY AS IT GOVERNS YOUR PROCESSING OF PERSONAL DATA WHEN USING THE ATLAN PLATFORM LICENSED VIA THE ORDER FORM SIGNED BY THE PARTIES. FOR THE PURPOSE OF THIS DPA, THE TERM "ATLAN" REFERS TO THE ATLAN CONTRACTING ENTITY MENTIONED IN THE ORDER FORM AND SIMILARLY THE TERM "CUSTOMER" SHALL REFERS TO THE CUSTOMER CONTRACTING ENTITY THAT SIGNED THE ORDER FORM.

In view of the foregoing, the parties hereby agree as follows:

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 clause shall have the meanings ascribed to them in the Data Protection Laws.

"Data Controller"	shall mean the means an entity that determines the purposes and means of the Processing of Personal Data.
"Data Protection Laws"	shall mean all applicable data protection and privacy laws applicable to the Controller 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**"), and any amending or replacement or equivalent legislation 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 data;
"**Data Processor**"	shall mean an entity that Processes Personal Data on behalf of a Data Controller and shall include the meaning ascribed to "service provider" under CCPA and/or "Data Intermediary" as the meaning is ascribed under SPDPA. In the case of this DPA, Data Processor shall refer to Atlan and its Affiliates (as defined in the Agreement) providing Services to Customer.
"**Data Subject**"	means the identified or identifiable natural person to whom the Personal Data shared with the Processor under this DPA relates.
"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.

"**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.
"Purposes"	shall include provision of Services by the Processor to the Controller as described in the Agreement, including without limitation, any Processing initiated by Users (as defined in the Agreement) in their use of the Services (as defined in the Agreement) and as further documented and basis reasonable instructions from Controller as agreed by the parties.
"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
"**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
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.
"Sub-processor"	shall mean any downstream processors used by the Data Processor to Process Personal Data while providing the Services to the Data Controller.
"Supervisory Authority"	shall mean the relevant supervisory 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 Purposes and only as instructed by the Customer. 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 10 b. of the Agreement.

b. Terms applicable to Personal Data subject to SPDPA. In the event SPDPA is applicable to the Processing carried out under this DPA, the Data Processor agrees and acknowledges that it is prohibited from selling any Personal Data received pursuant to the Purposes of this DPA unless otherwise permitted by SPDPA.

c. Terms applicable Personal Data subject to CCPA. If Customer uploads Customer Personal Data to the Service which is governed by CCPA, then the below clauses shall additionally apply in relation to Data Processor's role as a service provider for such Customer Personal Data:
   i. Data Processor shall not sell or share Customer Personal Data except as agreed by the parties;
   ii. Data Processor shall process Customer Personal Data only to the extent required to provide the Services, including without limitation, any support services provided by the Data Processor for which it may need to access Customer Personal Data. Data Processor shall not retain, use, or disclose the Customer 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 CCPA and its regulations;
   iii. Data Processor shall notify Customer no later than five (5) business days after it determines that it can no longer meet its obligations under CCPA and its regulations. Upon such notice, Customer may direct the Data Processor to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data by deleting all or the relevant portion of Customer Personal Data from the Service or by such other means as agreed between the parties.

d. Categories of Data Subjects. The categories of Data Subjects to whom the Personal Data relates shall be solely determined and controlled by the Customer (including where the Data Processor may be a sub-processor) and shall include, without limitation, the Personal Data required for User credentials.

e. Categories of Personal Data. The categories of Personal Data to be Processed by the Data Processor shall be solely determined and controlled by the Customer (including where the Data Processor may be a sub-processor) and could include, without limitation, contact details (name, email IDs, address), financial information, IT information and where applicable, Special Categories of Personal Data.

f. Retention of Personal Data. Any Personal Data Processed pursuant to the Agreement shall be retained until required for the Purposes described in this DPA. 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 Purposes of this DPA. The list of Data Processor's current Sub-processors is attached herewith as Schedule 1.

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 Schedule 1**. Any changes to Schedule 1 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 Clause 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 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.

V. 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.

VI. 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 Clauses 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, the parties shall enter into the applicable Standard Contractual Clauses (Controller to Processor or Processor to Processor in case the Data Processor is Customer's Sub-processor) and incorporated by reference.

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.

VII. 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.

VIII. 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.

IX. 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. Audits will be conducted by the Customer and/or its representative after providing a reasonable prior notice of at least 15 days either at the Data Processor's premises or online via a remote access. The Customer hereby agrees that in exercising its audit rights under this clause, 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.

X. 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. The Data Processor may update this DPA from time to time at this link or a successor website designated by the Data Processor provided however that no such update shall materially diminish the privacy or security of Customer Personal Data.

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.

XI. 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).

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

SCHEDULE 1 – LIST OF SUB-PROCESSORS

Sub-Processor	Address	Purposes
Amazon Web Services. Cloud Storage Services/ Environment	As per location of Customer Personal Data	For the provision of storing Customer Data for the purpose of provision of agreed services.
Atlan Inc.	1000 N West Street Suite 1281-M #171 Wilmington, DE 19801	For the purpose of provision of agreed services as per access provided by the Data Controller.
Atlan Technologies Pvt. Ltd.	Saket District Centre, Next to Select City- Walk Mall, District Mall, Sector 6, Pushp Vihar New Delhi South Delhi DL 110017 IN	For the purpose of provision of agreed services as per access provided by the Data Controller
Atlan Pte. Ltd.	3 Coleman Street, #03-24 Peninsula Shopping Complex, Singapore (179804)	For the purpose of provision of agreed services as per access provided by the Data Controller

SCHEDULE 2 – TECHNICAL AND ORGANISATIONAL MEASURES FOR DATA PROTECTION AND SECURITY OF THE DATA

We currently observe the Security Measures described in this Annex 2. All capitalised terms not otherwise defined herein will have the meanings as set forth in the General Terms. For more information on these security measures, please refer to Atlan's SOC 2 Type II Report, HIPAA Report and Penetration Test Summaries, available at request.

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

In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the Atlan product(s). Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

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 unauthorised 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.

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. All such access is logged. Employees are granted access by role and by the principle of least privilege.

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

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios. Penetration tests are performed against the application layers and network layers of the Atlan technology stack.

Responsible disclosure: A responsible disclosure program invites and incentivises 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 defences against sophisticated attacks.

Measures for user identification and authorisation

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorisation: 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 authorisation 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 centres. 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 designed our infrastructure to log extensive information about the system behaviour, traffic received, system authentication, 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 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 phishing emails.

Measures for certification/assurance of processes and products

We engage an external auditor to perform audits and provide attestations that we comply with SOC 2 Type II and HIPAA requirements.

Measures for ensuring data minimisation

We only persist metadata on data assets. We pass-through raw data from tables for our Preview and Query features to end users, but this data is not persisted in the platform. Customer is in complete control of the metadata and raw data that the Atlan application has access to.

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 Grievance Officer and 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://atln.cm/pvcy.