DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Master Agreement ("**Agreement**") under which the Provider entity provides Services for software and professional products. All capitalized terms not defined in this DPA will have the meaning given to them in other parts of the Agreement.

1. Definitions and Interpretation

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of a Covered Jurisdiction, and (b) is permitted to use the Services pursuant to the Agreement between Provider and Customer but has not signed its own Order Form with Provider and is not a "Customer" as defined under the Agreement.

"**Covered Jurisdiction**" means a cross-border processing of Personal Data that is restricted by Data Protection Laws because the disclosure is made to a person or entity located in a jurisdiction in which the applicable competent government authority or Data Processor determines does not ensure the same or higher level of data protection as the jurisdiction from which the Personal Data originates.

"**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Service(s) or whose Personal Data is Processed in the Service(s).

"**Data Processor**" means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the Provider entity that is a party to the Agreement.

"**Data Protection Laws**" means all applicable laws and regulations regarding the Processing of Personal Data, which may include without limitation and each as amended, superseded, or replaced: the Argentina Personal Data Protection Act (***ARGENTINA***); the Australia Privacy Act 1988 and 13 Australian Privacy Principles (***AUSTRALIA***); the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (***CA, USA***); the Canada Personal Information Protection and Electronic Documents Act 2000 and the Quebec Private Sector Act, Law 25 (***CANADA***); People's Republic of China Personal Information Protection Laws (***CHINA***); the Dubai International Financial Centre Data Protection Laws and Regulations (***DUBAI***); European Union General Data Protection Regulation (EU) 2016/679 (***EUROPEAN UNION***); the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong) (***HONG KONG***); the India Information Technology Rules 2011 and the Digital Personal Data Protection Act, 2023 (***INDIA***); the Japan Personal Information Protection Act (Kojin Joho no Hogo ni Kansuru Houritsu, Law No. 57 of 2003) (***JAPAN***); the Malaysia Personal Data Protection Act 2010 (***MALAYSIA***); the Mexico Federal Law on the Protection of Personal Data (***MEXICO***); the New Zealand Privacy Act 2020 (***NEW ZEALAND***); the Philippines Data Privacy Act 2012 (***PHILIPPINES***); the Saudi Arabia Personal Data Protection Law 2021 (***SAUDI ARABIA***); the Singapore Personal Data Protection Act 2012 (***SINGAPORE***); the South Africa Protection of Personal Information (2021) (***SOUTH AFRICA***); the Swiss Federal Act on Data Protection of 25 September 2020 ***(SWITZERLAND)***; the Turkey Law No. 6698 on the Protection of Personal Data (**TURKEY**); the United Arab Emirates Personal Data Protection Law 2021 (***UAE***); and the United Kingdom Data Protection Act 2018 and the UK General Data Protection Regulation (***UNITED KINGDOM***).

"**Data Subject**" means an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.

"**Personal Data**" means any information relating to an identified or identifiable Data Subject uploaded by or for Customer to the Services as Customer Data.

"**Processing, processes, and process**" means any activity that involves the use of Personal Data, or as the relevant Data Protection Laws may otherwise define the terms processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

"**Security Breach**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of or access to Personal Data.

"**Sub-Processor**" means any legal person or entity engaged in the Processing of Personal Data by Data Processor.

2. Nature, Scope and Purpose of the Processing

2.1 In performing the Services, Provider will comply with Provider's Privacy Policy, which is available at https://gomomentus.com/privacy-policy and incorporated herein by reference. Provider's Privacy Policy is subject to change at Provider's discretion; however, Provider's policy changes will not result in a material reduction in the level of protection provided for Personal Data provided as part of the Services under the Agreement.

2.2 The Customer and the Provider acknowledge that for the purpose of any applicable Data Protection Laws, the Customer is the Data Controller and the Provider is the Data Processor.

2.3 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Laws, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

2.4 Provider will only Process Personal Data in accordance with Customer's instructions and to the extent necessary for providing the Services. Customer acknowledges all Personal Data it instructs Provider to Process for the purpose of providing the Services must be limited to the Customer Data Processed within the Service. Details of the Processing of Personal Data conducted under this DPA are set forth in Schedule A.

2.5 The parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, if applicable, on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Provider and each such Authorized Affiliate subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is a party only to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

3. Data Processing Measures

3.1 Where Provider believes compliance with Customer's instructions would result in a violation of Data Protection Laws or is not in the ordinary course of Provider's obligations in operating Services, Provider will promptly notify Customer thereof.

3.2 Persons authorized by Provider to Process Personal Data will be bound by appropriate confidentiality obligations. Provider has appointed a data protection officer. The appointed person may be reached at privacy@gomomentus.com.

3.3 The Provider must at all times implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, unavailability, destruction, or damage. For certain Services, Provider also makes available security features and controls that Customer can elect to use. Customer is responsible for implementing any optional technical and organizational measures to protect Customer Data, as described in the Agreement or Documentation.

3.4 The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Laws, while also considering the nature of the Provider's processing and the information available to the Provider.

4. Security & Breach Notification

4.1 The Provider will immediately notify the Customer if it becomes aware of any advance in technology and methods of working, which indicate that the parties should adjust their security measures.

4.2 The Provider must take reasonable precautions to preserve the integrity of any Personal Data it processes and to prevent any corruption or loss of the Personal Data. The Provider Systems are programmed to perform routine daily data backups as set out in Provider's backup policy in effect from time to time. Provider will deliver to Customer its then most current back-ups of Customer Data. In the event of any loss, destruction, damage, or corruption of Customer Data caused by the Provider Systems or Services, Provider will, as its sole obligation and liability and as Customer's sole remedy, use commercially reasonable efforts to restore the Customer Data from Provider's then most current backup of such Customer Data.

4.3 Provider will report to Customer any Security Breach without undue delay following determination by Provider that a Security Breach has occurred.

4.4 The initial report will be made to Customer's security or privacy contact(s) designated in Provider's customer support portal (or if no such contact(s) are designated, to the primary technical contact designated by Customer). As relevant information in relation to the Breach is collected or otherwise becomes available to Provider, it will provide such information without undue delay to Customer, to assist Customer to comply with its notification obligations under Data Protection Laws. In particular, and to the extent reasonably possible and applicable, Provider will provide Customer with the information described in Article 33 of GDPR.

4.5 Customer will cooperate with Provider in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any Security Breaches, identify its root cause(s) and prevent a recurrence. Customer, as the Data Controller, is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects in relation to any Security Breach and for providing such notice.

5. Requests from Data Subjects and Authorities.

5.1 During the Term, Provider will provide Customer with the ability to access, correct, rectify, erase, or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under the applicable Data Protection Laws (collectively, "**Data Subject Requests**").

5.2 Customer will be solely responsible for responding to Data Subjects in respect of any Data Subject Requests, provided that Provider will reasonably cooperate with Customer in relation to Data Subject Requests to the extent Customer is unable to fulfill such Data Subject Requests using the functionality in the Services. Provider will instruct the Data Subject to contact the Customer in the event it receives a Data Subject Request directly.

5.3 In the case of a notice, audit, inquiry, or investigation by a government body, data protection authority, or law enforcement agency regarding the Processing of Personal Data, Provider will promptly notify Customer unless prohibited by applicable law. Each party will cooperate with the other party by providing all reasonable information requested and available.

6. Audits.

6.1 Provider will allow for and contribute to audits that include inspections by granting Customer access to reasonable and industry recognized documentation evidencing the policies and procedures governing the security and privacy of Personal Data ("**Audit**"). The information available in an Audit will include documentation evidencing the privacy policies and procedures regarding Personal Data Processed, as well as copies of any certifications and attestation reports that exist at such times (including audits). To the extent that Customer has not reasonably been able to satisfy its audit requirements by following the procedure outlined in this Clause, Provider will provide Customer with such further assistance as may reasonably be required (in accordance with the assistance obligations described herein) to substantially satisfy such requirements.

6.2 Upon Customer's request by emailing privacy@gomomentus.com, Provider and Customer may schedule a mutually convenient time to discuss the Audit. In the event the Audit has any findings of material noncompliance with the DPA, then Provider will promptly address such findings of noncompliance. Provider may, in its sole discretion and consistent with industry and Provider's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Provider's security program. The Audit and the results derived therefrom are Confidential Information of Provider.

7. Sub-Processors.

7.1 Customer acknowledges and agrees that (a) Provider's Affiliates may be retained as Sub-Processors; and (b) Provider and Provider's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Provider or a Provider Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor. The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed on Schedule B, which may be updated from time to time or in accordance with Clause 7.2. Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data.

7.2 For Covered Jurisdictions, prior to Provider engaging a new Sub-Processor for the Services, Provider will: (a) notify Customer by email to Customer's designated contact in Provider's support portals or accounts (or other mechanism used to notify its customer base); and (b) have such Sub-Processor enter into a written agreement with Provider (or the relevant Provider Affiliate) requiring the Sub-Processor to abide by terms no less protective than those provided in this DPA. With respect to providing the notice described in the preceding sentence, Provider will provide at least 30 days' prior written notice before engaging a Sub-Processor with respect to existing Services which Customer has purchased. If a new Sub-Processor is engaged to support a new Service or a new feature of an existing Subscription Service, then the notice described in this

Clause will be provided at or before the time such feature or Subscription Service is made generally available. Upon written request by Customer by emailing privacy@gomomentus.com, Provider will make a summary of the data processing terms with the Sub-Processor available to Customer. Customer may request in writing by emailing privacy@gomomentus.com reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.

7.3 Customer may object to Provider's use of a new Sub-processor by notifying Provider promptly in writing within thirty (30) days of receipt of Provider's notice in accordance with the mechanism set out in Clause 7.2. If Customer objects to a new Sub-processor as permitted in the preceding sentence, Provider will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Provider is unable to make available such change within a reasonable period of time after both parties have engaged in good faith, which shall not exceed ninety (90) days, Customer may upon thirty (30) days prior notice terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Provider without the use of the objected-to new Sub-processor. The Customer's right to terminate the relevant Services under this clause will not relieve Customer of any payment obligations under the Agreement up to the date of termination. If the termination in accordance with this clause only pertains to a portion of services under an Order Form, Customer agrees to enter into an amendment or replacement order to reflect such partial termination.

7.4 Use of a Sub-Processor will not relieve, waive, or diminish any obligation of Provider under this DPA, and Provider is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Provider.

8. Limitation of Liability & Term.

8.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Provider, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Provider's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

8.2 This DPA will remain in full force and effect so long as the Term of the Agreement remains in effect or the Provider retains any Personal Data related to the Agreement in its possession or control. In the event of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter herein, this DPA shall control. The primary Data Processor is a United States company and therefore the standard version of the DPA is the English version. In case of misinterpretation due to translation of the documents in either French or German, the English version always prevails.

9. International Data Transfers.

9.1 The transfer of Personal Data from a Covered Jurisdiction to a country which is not located in a jurisdiction that is subject to a valid adequacy decision (as determined by the applicable Data Protection Laws regarding the individuals about whom the Personal Data is Processed) (a "**Data Transfer**") will be subject to the standard contractual clauses of the SCCs below, subject to any necessary adjustments for compliance with the applicable Data Protection Laws. For all Services, Personal Data will be stored/hosted in the data center

region specified in the Order Form/Agreement for such Services or, if applicable, the geographic region that was selected when activating the production instance of such Services. Notwithstanding such storage/hosting requirements and subject to this DPA, Provider may process Personal Data globally as necessary to perform the Services, such as for support, incident management or data recovery purposes.

9.2 EEA Data Protection Law.

(a) If there is a Data Transfer subject to Data Protection Laws of the EEA, the Data Transfer will be subject to the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as annexed to Commission Implementing Decision 2021/914 and any updates thereto ("**SCCs**"), which are incorporated into this DPA by this reference.

(b) **SCCs Modules**. Module Two (Data Controller to Data Processor) will apply to a Data Transfer when Customer is a Data Controller. Module Three (Data Processor to Data Processor) will apply to a Data Transfer when Customer is a Data Processor.

(c) **SCCs Optional Provisions**. Where the SCCs identify optional provisions:

(i) Clause 7 (Docking Clause) – the optional provision shall be deemed incorporated and applied;

(ii) Clause 8.3 – Before disclosing a copy of the SCCs pursuant to Clause 8.3, the disclosing party must use commercially-reasonable efforts to redact all commercial terms but provide a meaningful summary if the data subject would otherwise not be able to understand the content or exercise his/her/their rights as a result of the redaction;

(iii) Clause 9(a) (Use of sub-processors) – Option 2 applies (and the parties will follow the process and timings agreed in the DPA to appoint sub-processors);

(iv) Clause 11(a) (Redress) – the optional provision does not apply;

(v) Clause 12 – any claims brought under the SCCs shall be subject to the terms and conditions set forth in the Agreement. In no event shall any party limit its liability with respect to any Data Subject rights under the EU SCCs;

(vi) Clause 17 (Governing law) – option 1 applies, and where the Agreement is governed by the laws of an EU Member State, the laws of that EU Member State apply; otherwise, Irish law applies; and

(vii) Clause 18(b) (Choice of forum and jurisdiction) – where the Agreement is subject to the jurisdiction of the courts of an EU Member State, the courts of that EU Member State have jurisdiction; otherwise, the courts of Dublin, Ireland have jurisdiction.

(d) **Annexes of SCCs.**

(i) Annex 1A: the data exporter(s) is the Customer and its Affiliates making the Data Transfer (the "**Data Exporter**") and the data importers are Provider entities receiving the Data Transfer (the "**Data Importer**"). The full name, address and contact details for the Data Exporter and the Data Importer are set out in the Agreement or can be requested by either party.

(ii) Annex 1B: The relevant details are those set out in the Agreement, including Schedule 1 "Details of Processing" of this DPA.

(iii) Annex 1C: The competent supervisory authority is the supervisory authority applicable to the Customer (or, where relevant, applicable to the Customer's representative).

(iv) Annex 2: the security provisions contained in Addendum 1 or other security related provisions in the Agreement apply.

(e) **Notices**. All notices, requests, monitoring/audit rights, conduct of claims, liability, and erasure or return of data relating to the SCCs will be provided/managed/interpreted, as applicable, in accordance with the relevant provisions in the Agreement, to the extent that such provisions do not conflict with the SCCs.

9.3 Switzerland Data Protection Law.

(a) If there is a Data Transfer subject to Data Protection Laws of Switzerland, then the SCCs will apply with the following modifications:

(i) references to "GDPR" in the SCCs will be understood as references to Data Protection Laws of Switzerland ("**FADP**");

(ii) references to a "Member State" and "EU Member State" will not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and

(iii) the competent supervisory authority in Annex 1.C under Clause 13 will be the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**"). However, where the Personal Data transferred is subject to both the FADP and the SCCs, parallel supervision should apply: for the (revised) FADP, the FDPIC shall be the competent Supervisory Authority insofar as the transfer is governed by the (revised) FADP; and for SCCs, the competent Supervisory Authority is (a) the Supervisory Authority of the country where the Data Exporter is established if the Data Exporter is established in the EEA, or (b) the Supervisory Authority of Ireland if the Data Exporter is not established in EEA.

9.4 UK Data Protection Law.

(a) If there is a Data Transfer subject to Data Protection Laws of the United Kingdom, then the International Data Transfer Addendum to the SCCs ("**UK IDTA**"), as issued by the Information Commissioner in the United Kingdom will apply and is incorporated by reference into this DPA. The information needed to complete the Tables to the UK IDTA is set out in the Agreement, including Schedule 1 "Details of Processing" of this DPA.

(b) In Table 2 of the UK IDTA, parties select the checkbox that reads: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum", and the accompanying table shall be deemed to be completed according to the parties' preferences outlined in this DPA. For the purposes of the UK IDTA, the governing law shall be deemed to be that of England & Wales.

(c) In Table 4, the parties agree that either party may terminate the Addendum as set out in Clause 19 of the UK IDTA.

9.5 People's Republic of China Data Protection Law.

(a) If there is a Data Transfer subject to Data Protection Laws of the People's Republic of China, then Customer shall immediately notify Provider and take all necessary steps to minimize the amount of Personal Data shared with Provider.

(b) Any dispute arising from Data Protection Laws of the People's Republic of China shall be submitted to China International Economic and Trade Arbitration Commission (CIETAC) Shanghai Sub-Commission for arbitration, which shall be conducted in Shanghai in accordance with the CIETAC's arbitration rules in effect at the time of arbitration. All decisions made by the arbitral tribunal shall be final and binding upon the parties.

9.6 Argentina Data Protection Law.

(a) If there is a Data Transfer subject to Data Protection Laws of Argentina, then Provider and Customer hereby agree to the additional clauses set forth in the Annexes to Regulation No. 60-E/2016, available at https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm.

(b) Jurisdictions considered to provide an adequate level of data protection under the Data Protection Laws of Argentina include the members of the European Economic Area (EEA), Switzerland, Guernsey, Jersey, the Isle of Man, the Faroe Islands, Canada (only for the private sector), the Principality of Andorra, New Zealand, the Republic of Uruguay, the State of Israel (only for data that is subject to automated processing), and the United Kingdom of Great Britain and Northern Ireland.

9.7 Notwithstanding the fact that the SCCs and/or UK IDTA are incorporated herein by reference without the signature pages of the SCCs actually being signed by the data exporter or data importer, the parties agree that its respective execution of the Agreement is deemed to constitute its execution of the SCCs and/or the UK IDTA on behalf of the data exporter/data importer (as applicable).

9.8 If an alternative transfer mechanism, such as Binding Corporate Rules, is adopted by Provider, or the Trans-Atlantic Data Privacy Framework (an "**Alternative Mechanism**") becomes available during the term of the Agreement, and Provider notifies Customer that some or all Data Transfers can be conducted in compliance with Data Protection Laws pursuant to the Alternative Mechanism, the parties will rely on the Alternative Mechanism instead of the provisions above for the Data Transfers to which the Alternative Mechanism applies.

9.9 Provider may change this DPA if the change reflects a change in the name or form of a legal entity; and/or is necessary to comply with Data Protection Laws (including guidance issued by a data protection authority in a Covered Jurisdiction), or a binding regulatory or court order.

SCHEDULE A

Personal Data Processing Purposes and Details

1. Subject matter. The subject matter of the data processing under this DPA is the Personal Data included in Customer Data.

2. Duration. As between Provider and Customer, the duration of the data processing under this DPA is the Term under the Agreement.

3. Purpose and nature. The purpose and nature of the data processing under this DPA is the provision of the Services by Provider under the Agreement and applicable Order Forms.

4. Type of Personal Data. Personal Data included in Customer Data which is uploaded by Customer or Authorized Users to the Services.

5. Categories of data subjects. The data subjects could include Customer's employees, suppliers, agents, partners and/or end users as authorized in the Order Forms.

Data Security Measures

1. SECURITY PROGRAM

While providing the Service(s), Provider will ensure there is a written information security program of policies, procedures, and controls aligned to industry standards, governing the processing, storage, transmission, and security of Customer Data. The Security Program will include industry-standard processes and procedures designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Provider updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that no such update will materially reduce the overall level of commitments or protections provided to Customer as described herein.

1.1 SECURITY ORGANIZATION. There will be a Chief Information Security Officer, or equivalent executive, that is designated as responsible for coordinating, managing, and monitoring the information security function, policies, and procedures.

1.2 POLICIES. The information security policies will be: (i) documented; (ii) reviewed and approved by management, including after material changes; and (iii) published, and communicated to personnel, and contractors, including appropriate ramifications for non-compliance.

1.3 RISK MANAGEMENT. There will be information security risk assessments performed as part of a risk governance program that is established with the objective to regularly test, assess, and evaluate the effectiveness of the Security Program. Such assessments will be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

2. AUDITS

2.1 AUDIT. Provider will allow for and contribute to audits that include inspections by granting Customer access to reasonable and industry recognized documentation evidencing the policies and

procedures governing the security and privacy of Customer Data and the Security Program through a self-access documentation portal and at no additional cost. The information available in the portal will include documentation evidencing the Security Program, inclusive of the privacy policies and procedures regarding Personal Data Processed. To the extent that Customer has not reasonably been able to satisfy its audit requirements by following the procedure outlined in this Clause, Provider will provide Customer with such further assistance as may reasonably be required (in accordance with the assistance obligations described herein) to substantially satisfy such requirements.

2.2 OUTPUT. Upon Customer's request, Provider and Customer may schedule a mutually convenient time to discuss the Audit. In the event the Audit has any findings of material noncompliance with the Data Processing Addendum or this Data Security Measures (DSM), then Provider will promptly address such findings of noncompliance. Provider may, in its sole discretion and consistent with industry and Provider standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Provider's Security Program. The Audit and the results derived thereof are Confidential Information of Provider.

3. PHYSICAL, TECHNICAL, AND ORGANIZATIONAL SECURITY MEASURES

3.1 PHYSICAL SECURITY MEASURES.

3.1.1. DATA CENTER FACILITIES. The data center facilities will include: (1) physical access restrictions and monitoring that will include a combination of any of the following: multi-zone security, mantraps, appropriate perimeter deterrents, on-site guards, biometric controls, CCTV, and secure cages; and (2) fire detection and fire suppression systems both localized and throughout the data center floor.

3.1.2. MEDIA. For deletion of data, an industry standard such as NIST 800-88 or substantially equivalent will be used for the deletion of sensitive materials, including Customer Data, before final disposition of such media.

3.2 TECHNICAL SECURITY MEASURES.

3.2.1. ACCESS ADMINISTRATION. Access by personnel to Customer Data will be conducted in a manner that: (i) is protected by authentication and authorization mechanisms; (ii) requires personnel to be assigned a unique user account; (iii) restricts the sharing of individual user accounts; (iv) requires strong authentication with complex passwords; (v) ensures accounts are lock-out enabled; (vi) requires access over a VPN; (vii) requires access privileges be based on job requirements limited to that necessary for the applicable personnel to undertake their duties; (viii) ensures access is revoked upon termination of employment or consulting relationships; and (ix) requires access entitlements be reviewed by management quarterly.

3.2.2. LOGGING AND MONITORING. The production infrastructure log activities will be centrally collected, secured to prevent tampering, and monitored for anomalies by a trained security team.

3.2.3. FIREWALL SYSTEM. Firewall technology will be installed and managed to protect systems and inspect ingress connections. Managed firewall rules will be reviewed in

accordance with then-current operating procedures, which will be reviewed no less frequently than quarterly.

3.2.4. VULNERABILITY MANAGEMENT. Vulnerability scans will be performed within the environment to determine potential vulnerabilities in accordance with then-current security operating procedures, which will be at least quarterly. When software vulnerabilities are revealed and addressed by a vendor patch, the patch will be obtained from the applicable vendor and applied within an appropriate risk-based timeframe in accordance with the then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in production systems.

3.2.5. ANTIVIRUS. Antivirus, anti-malware, and anti-spyware software will be updated on regular intervals and centrally logged.

3.2.6. CHANGE CONTROL. Changes to the environment will be reviewed to minimize risk. Such changes will be implemented in accordance with the current standard operating procedure.

3.2.7. CONFIGURATION MANAGEMENT. Standard hardened configurations for the system components within the environment will be maintained using industry standard hardening guides, such as guides from the Center for Internet Security.

3.2.8. DATA ENCRYPTION IN TRANSIT. Industry standard encryption will be used to encrypt Customer Data in transit over public networks.

3.2.9. DATA ENCRYPTION AT REST. Data drives on servers holding Personal Data and attachments use full disk, industry-standard, AES-256 encryption at rest.

3.2.10. ILLICIT CODE AND SECURE SOFTWARE DEVELOPMENT. Provider will follow the secure software development and code review practices described in this clause to prevent harm from malware, such as from viruses, worms, date bombs, time bombs, or shut down devices. Software will be developed using secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten or a substantially equivalent standard. Personnel responsible for secure application design and development will receive appropriate training regarding secure application development practices.

3.2.11. SECURE CODE REVIEW. A combination of static and dynamic testing of code will be performed prior to the release of such code to Customers. Vulnerabilities will be addressed in accordance with the then-current software vulnerability management program. To address vulnerabilities where code has been made available to Customers, software patches will be regularly made available to Customers.

3.3 ORGANIZATIONAL SECURITY MEASURES.

3.3.1. PERSONNEL SECURITY. Background screening will be performed on all employees and all contractors who have access to Customer Data in accordance with applicable standard operating procedure and subject to applicable Law.

3.3.2. SECURITY AWARENESS AND TRAINING. Security and Privacy awareness training and education will be provided to employees and contractors who have access to Customer Data. Such training will be conducted at time of hire and at least annually throughout employment.

3.3.3. VENDOR RISK MANAGEMENT. Any vendor that accesses, stores, processes, or transmits Customer Data will be assessed to ensure it has appropriate security and privacy controls.

3.3.4. SOFTWARE AND ASSET INVENTORY. An inventory of the software components including, but not limited to, open-source software used in the environment will be maintained.

3.3.5. WORKSTATION SECURITY. Security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption with a minimum of AES 256-bit encryption will be implemented and maintained. Personnel will be restricted from disabling security mechanisms.

4. SERVICE CONTINUITY

4.1 DATA LOCATION. Provider will host the subscribed instances in data centers located in the default geographic region specified on DPA or otherwise specified in the contractual agreement, which have attained SOC2 Type 2 attestations, ISO 27001 certifications, or equivalent or successor attestations/certifications.

4.2 DATA BACKUP. Back-ups will be performed of all Customer Data in accordance with the current operating procedure published in the portal.

4.3 DISASTER RECOVERY. A Business Continuity/Disaster Recovery Plan (BC/DRP) to address disaster recovery will be maintained that is consistent with industry standards for the environment and will: (i) include processes for protecting personnel and assets (ii) test the BC/DRP at least once every year; (iii) make available summary test results that will include the actual recovery point and recovery times; and (iv) document any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the environment from being recovered in accordance with the BC/DRP .

5. MONITORING AND INCIDENT MANAGEMENT

5.1 INCIDENT MONITORING AND MANAGEMENT. System events are monitored and analyzed in a timely manner in accordance with Provider's current standard operating procedures. Incident response teams will be escalated to and engaged as necessary to address a security incident.

5.2 BREACH NOTIFICATION.

5.2.1. NOTIFICATION. Provider will report to the Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of or access to Customer Data without undue delay following determination by Provider that a Breach has occurred.

5.2.2. REPORT. The initial report will be made to Customer's security, privacy, or the primary technical contact designated by Customer. As relevant information in relation to the Breach is collected or otherwise becomes available to Provider, it will provide such

information without undue delay to the Customer, to assist Customer to comply with its notification obligations under Data Protection Laws. To the extent reasonably possible and applicable, Provider will provide the Customer with the information described in Article 33 of GDPR.

5.2.3. DATA CONTROLLER OBLIGATIONS. The Customer will cooperate with Provider in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence. The Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects in relation to any Breach and for providing such notice.

6. PENETRATION TESTS

6.1 BY A THIRD-PARTY. Provider will engage skilled third-party vendors to perform penetration on the Provider application and platform to identify vulnerabilities. Executive reports from the penetration testing are made available to Customers in the portal.

6.2 BY CUSTOMER. Customer may request to perform, at its own expense, a web penetration test on hosting environments in which Customer Data is stored; provided that Customer will: (i) notify Provider and submit a request to schedule such a test using the Support Portal. In the event Customer's authorized penetration testing identifies vulnerabilities that Provider is able to reproduce, Provider will, consistent with industry-standard practices, use commercially reasonable efforts to promptly make any necessary changes to improve the security of the Service.

7. SHARED SECURITY RESPONSIBILITY

7.1 PRODUCT CAPABILITIES. Provider provides a variety of security settings that allow Customer to configure security of the Services for their own use such as, but not limited to: (i) authenticate users before accessing the Customer's instance; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) access instance application logs. Customer will manage each user's access to and use of the Services by assigning to each user a credential and user type that controls the level of access to the applicable Services. Customer bears sole responsibility for reviewing the Security Program and making an independent determination as to whether it meets Customer's requirements, considering the type and sensitivity of Customer Data that Customer provides to Provider. Customer bears sole responsibility for protecting the confidentiality of each user's login and password and managing each user's access to the Services.

7.2 SECURITY CONTACT. Customer agrees to identify and maintain appropriate security contact(s) for all information security incident and information security-related communication within the Support Portal.

7.3 LIMITATIONS. Notwithstanding anything to the contrary in this DSM or other parts of the Agreement, Provider's obligations herein are only applicable to the Services. This DSM does not apply to: (i) information shared with Provider that is not Customer Data; (ii) data in Customer's VPN or a third-party network; and (iii) any data processed by the Customer or its users in violation of the Agreement or this DSM.

SCHEDULE B

Sub-processor / Country	Services
Amazon Web Services, Inc. ("AWS") United States of America; Australia; Canada; Ireland (EU); Singapore; and United Kingdom	Cloud hosting service
Microsoft Corporation United States of America, Ireland, Canada, and Australia	Cloud hosting service
Microsoft Corporation United States of America	Outlook calendar integration
Nournet Company Saudi Arabia	Cloud hosting service in Saudi Arabia
Provider's Affiliates • Ungerboeck Systems International, LLC United States of America and New Zealand • Ungerboeck Software International, Pty Ltd. Australia and New Zealand • Oletha Pty Ltd India • Ungerboeck Systems International GmbH United Kingdom	Customer support related to contract execution and services
AC PM, LLC United States of America	Email service provider (Postmark)

Atlassian US, Inc. United States of America	Collaboration software platform
Caffeinated Corporation United States of America	Automated Customer support assisted by AI to streamline and automate support
Datadog, Inc. United States of America	Network and Infrastructure performance monitoring
Delighted, LLC United States of America	Customer feedback management tool

DocuSign Inc., United States of America	Electronic Signature integration and envelope provisioning
Dynatrace, LLC, United States of America	Third-party monitoring and logging platform
Flowgear LLC, United States of America	Integration Platform as a Service
Google United States of America	SSO SAML 2.0, maps, and calendar integration
Jotform, Inc., United States of America	Online forms integration
Okta, Inc. United States of America	Identity provider
Pendo.io, Inc., United States of America	User analytics tool
Productboard, Inc., United States of America	Product tracking software
Signiant Inc., United States of America	Integration of Media Shuttle service for data transfer
Stripe, Inc., United States of America	Payment processor
Twilio, Inc. United States of America	Integration of SendGrid email solution
Validity, Inc United States of America	Data Integrity Platform
Wiz, Inc. United States of America	Cloud Security Platform
Zendesk, Inc. United States of America	Support center and knowledge base; Ticketing system for customer support tickets
Full Story, Inc. United States of America	User Analytics tool
CheifSight Corporation United States of America	Business Analytics tool
Fivetran, Inc. United States of America	Automated data movement platform.
Snowflake, Inc. United States of America	Cloud-based data warehouse platform
Gainsight, Inc. United States of America	Customer success and Product Experience Software
Thought Industries, Inc. United States of America	Customer learning platform

For Customers outside of the EU

Philo Labs France	Video messaging services (Birdie) for customer service teams