TERMS AND CONDITIONS

1. SERVICES AND SUPPORT

In consideration of (and subject to) payment of the fees and marketing obligations listed herein and on the applicable Order Form (the “Fees”) and subject to full compliance with all the terms and conditions of this Agreement, Service Provider will use reasonable commercial efforts to provide Customer the Services selected in the Order Form, the applicable General Service Level Support Terms identified in Exhibit A, and the Data Protection Addendum (the “DPA”) attached as Exhibit B. In the event of any conflict between the DPA and this Agreement, the DPA shall govern.

As part of the registration process, Customer will identify an administrative username and password for Customer’s Service Provider account (the “Account”). Customer may use the administrative username and password to create standard users (each with a user password). Service Provider reserves the right to (i) refuse registration; or (ii) cancel passwords; it reasonably deems inappropriate. By entering into this Agreement and using the Service, Customer accepts and agrees to be bound by the Service Provider’s terms of service as provided herein, and privacy policies listed on Service Provider’s website. Service Provider shall notify Customer of any material changes to either of the foregoing policies.

2. RESTRICTIONS AND RESPONSIBILITIES

2.1 This is a contract for Services and the applicable hosted software will be installed, accessed and maintained only by or for Service Provider and no license is granted thereto. Subject to all terms of this Agreement, Service Provider hereby grants to Customer and its Affiliates, for the term of this Agreement, a worldwide, non-exclusive, non- sublicensable, non-transferable, non-assignable, fully paid for, royalty free license to use, reproduce and distribute internally within Customer’s and its Affiliates’ business, and for Customer’s and its Affiliates’ internal use only (and only in accordance with any applicable documentation provided to Customer and its Affiliates by Service Provider), the documentation and data provided to Customer and its Affiliates by Service Provider (the “Customer Data”). Customer and its Affiliates will not (and will not allow any third party to), directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the Services (or any underlying software, documentation or data related to the Services); modify, translate, or create derivative works based on the Services or any underlying software; or copy (except for archival purposes), rent, lease, distribute, pledge, assign, or otherwise transfer or encumber rights to the Services or any underlying software; use the Services or any underlying software for timesharing or service bureau purposes or otherwise for the benefit of a third party; publish the Customer Data without the prior written consent of Service Provider; or remove any proprietary notices or labels. For

purposes of this Agreement, “Affiliates” means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer, where “control” means ownership of at least 50% of the voting securities or other ownership interest.

2.2 Customer represents, covenants, and warrants that Customer will access and use the Services only in compliance with Service Provider’s standard access and security policies provided to Customer by Service Provider in writing. Customer shall be responsible for obtaining and maintaining any equipment and ancillary services reasonably needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, server, software, operating system, networking, web servers and telephone service (collectively, “Equipment”). Customer shall be responsible for compliance with any and all applicable third-party terms of service and privacy policies for platforms, networks and/or websites that they run their applications on, including but not limited to, Facebook, Android or iOS App Store.

2.3 Customer shall be responsible for ensuring that such Equipment is compatible with the Services and complies with all configurations and specifications set forth in Service Provider’s policies provided to Customer by Service Provider. Customer shall also be responsible for maintaining the security of the Equipment, the Account, passwords (including but not limited to administrative and user passwords) and files, and for all uses of the Account or the Equipment with or without Customer’s knowledge or consent, provided however, that Customer shall have no liability or responsibility for acts or omissions, in its Account or otherwise, to the extent those were enabled by Services Provider’s negligence, willful misconduct, or system failures.

2.4 Upon prior written approval by Customer after Customer’s successful use of the Service for at least six months, Service Provider may (i) produce and publish a case study on its website regarding the Customer’s use of the Services, and (ii) create self-promotional materials such as advertisements, brochures, etc. Upon prior written approval by Customer after Customer’s successful use of the Service for at least six months, Customer may provide a mutually agreeable quote with respect to Service Provider and the Services, to be used for Service Provider’s marketing and publicity purposes.

CONFIDENTIALITY AND PROPRIETARY RIGHTS

3.1 Each party (the “Receiving Party”) understands that the other party (the “Disclosing Party”) has disclosed or may disclose information relating to the Disclosing Party’s business (hereinafter referred to as “Proprietary Information” of the Disclosing Party). Proprietary Information of the Service Provider includes Services underlying software, algorithms and information embodied therein (hereinafter referred to as “Proprietary Information of the Service Provider”), and Proprietary Information of the Customer includes non- public data, any materials provided by Customer to the Service Provider to enable the provisions of the Services either it is

or was disclosed in tangible or written form, and the existence of this transaction (hereinafter referred to as “Proprietary Information of the Customer”).

3.2 Service Provider is granted a non-exclusive, non-transferable, non- sublicensable, royalty-free license to use the Proprietary Information of the Customer solely in connection with the provision of the Services under this Agreement.

3.3 The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary Information, and (ii) not to use (except as expressly permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after three (3) years following the disclosure thereof (except the Services and underlying software, algorithms and information embodied therein which shall remain confidential indefinitely) or any information that the Receiving Party can show evidence that (a) is or becomes generally available to the public, or (b) was in its possession or known by it without restriction on disclosure prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party, or (e) is required by law to be disclosed, under a specific legal order. Notwithstanding anything to the contrary, Service Provider shall have the right collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning Customer usage data derived therefrom), and Service Provider will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Service Provider, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business.

PAYMENT OF FEES

4.1 Customer will pay Service Provider the Fees for the Services as listed on the Order Form. The fees for any renewal term shall be at Service Provider’s then standard rates currently in effect, or if applicable, as otherwise stated in the Order Form.

4.2 If Customer believes that Service Provider has billed Customer incorrectly, Customer must contact Service Provider no later than sixty (60) days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Service Provider’s customer support department. Service Provider shall respond to Customer within three (3) business days after receiving such inquiries.

4.3 Service Provider shall bill through an (i) online payment form; or (ii) invoice, payment for which must be received by Service Provider within thirty (30) days of Customer's receipt of such invoice, or the Services may be terminated. Unpaid invoices are subject to a finance charge of 0.5% per month on any outstanding balance, or the maximum permitted by law, whichever is lower, plus all reasonable expenses of collection. Customer shall be responsible for all taxes associated with Services.

TERMINATION

5.1 Subject to earlier termination as provided below, this Agreement is for the initial Service Term as specified in the applicable Order Form (the "Initial Service Term"). This Agreement is not subject to any implied or automatic renewals.

5.2 In addition to any other remedies it may have, each party may also terminate this Agreement upon thirty (30) days' notice if the other party materially breaches any of the terms or conditions of this Agreement, and if the breach is capable of remedy, fails to promptly remedy that breach within twenty one (21) days of notice. If this Agreement is terminated as a result of a material breach by Customer during the Initial Service Term, Customer will pay in full all remaining Fees payable through the remainder of the Initial Service Term. If this Agreement is terminated as a result of an uncured material breach by Service Provider, Service Provider shall promptly refund to Customer any prepaid and unused Fees. If this Agreement is terminated as a result of a material breach by Customer after the Initial Service Term, the Customer will pay in full for any earned, but unpaid Services, pro-rated up to and including the last day on which the Services are provided.

5.3 Termination (which includes expiration or non-renewal) of this Agreement shall not limit either party from pursuing other remedies available to it, including injunctive relief, nor shall such termination relieve Customer's obligation to pay all undisputed fees that have accrued or are otherwise owed by Customer for Services provided in full, under any order form.

5.4 The parties' rights and obligations under Sections 2 ("Restrictions and Responsibilities"), 3 ("Confidentiality"), 4 ("Payment of Fees"), 6 ("Indemnification"), 7 ("Warranty and Disclaimer"), 8 ("Limitation of Liability"), and 9 ("Miscellaneous") shall survive termination.

INDEMNIFICATION

6.1 Service Provider agrees, at its own expense, to indemnify, defend Customer and hold Customer harmless against any suit, claim, or proceeding brought against Customer alleging that the use of Services in accordance with this Agreement infringes any copyright, trademark or

patent, provided that Customer (i) promptly notifies Service Provider in writing of any such suit, claim or proceeding, such notice to be considered prompt except to the extent the Service Provider is materially prejudiced by its delay (ii) allows Service Provider, at Service Provider's own expense, to direct the defense of such suit, claim or proceeding, and (iii) gives Service Provider all information and assistance reasonably necessary to defend such suit, claim or proceeding. The foregoing obligations do not apply with respect to the Services or portions or components thereof (x) not supplied by Service Provider, (y) made in whole or in part in accordance to Customer specifications, (z) combined with other products, processes or materials where the alleged infringement would not have occurred without such combination. This section states Service Provider's entire liability and Customer's exclusive remedy for infringement or misappropriation of intellectual property of a third party.

WARRANTY AND DISCLAIMER

7.1 SERVICE PROVIDER REPRESENTS AND WARRANTS THAT FOR THE TERM OF THIS AGREEMENT THE SERVICES SHALL BE PROVIDED IN A COMPETENT AND WORKMANLIKE MANNER, FREE OF MATERIAL DEFECTS. SERVICE PROVIDER FURTHER WARRANTS THAT: (A) THE SERVICES INCLUDING ANY RELATED SOFTWARE WILL PERFORM MATERIALLY IN ACCORDANCE WITH THE APPLICABLE DOCUMENTATION OR SPECIFICATIONS DURING THE AGREEMENT TERM, (B) SERVICE PROVIDER SHALL MAKE COMMERCIALLY REASONABLE EFFORTS TO MAKE THE SOFTWARE AVAILABLE TO CUSTOMER 24 HOURS A DAY, 7 DAYS A WEEK, AND (C) SERVICE PROVIDER WILL EMPLOY THEN- CURRENT, INDUSTRY-STANDARD MEASURES TO TEST THE SERVICES TO DETECT AND REMEDIATE VIRUSES, TROJAN HORSES, WORMS, LOGIC BOMBS, OR OTHER HARMFUL CODE OR PROGRAMS DESIGNED TO NEGATIVELY IMPACT THE OPERATION OR PERFORMANCE OF THE SOFTWARE.

7.2 SUBJECT TO THE GENERAL SERVICE LEVEL SUPPORT TERMS ATTACHED, SERVICE PROVIDER DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE OR MEET CUSTOMER'S REQUIREMENTS; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. THE SERVICES ARE PROVIDED "AS IS" AND SERVICE PROVIDER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

LIMITATION OF LIABILITY.

NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON OR GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, A BREACH OF EITHER PARTY'S CONFIDENTIALITY OBLIGATIONS UNDER SECTION 3, OR A BREACH OF

PRIVACY BY CYMON AI OR ITS SUBPROCESSORS, NEITHER PARTY SHALL BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS OR PROFITS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY FORCE MAJEURE EVENT OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED FEES PAID OR PAYABLE BY CUSTOMER TO SERVICE PROVIDER FOR THE APPLICABLE SERVICES UNDER THIS AGREEMENT OR RELATING TO ANY SUBJECT MATTER OF THIS AGREEMENT IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY.

MISCELLANEOUS

If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. This Agreement is not assignable, transferable or sublicensable except (i) as otherwise provided herein; (ii) with the other party's prior written consent; or (iii) a party may assign this Agreement to its successor in interest by way of a merger, acquisition, or sale of all or substantially all of its assets without consent. No agency, partnership, joint venture, or employment is created as a result of this Agreement and neither party has any authority of any kind to bind or attempt to bind the other party in any respect whatsoever. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. The parties agree that any material breach of Section 2 or 3 may cause irreparable injury and that each party may seek injunctive relief in a court of competent jurisdiction will be appropriate to prevent an initial or continuing breach of Section 2 or 3 in addition to any other relief to which the owner of such Proprietary Information may be entitled. This Agreement shall be governed by the laws of the State of New Jersey without regard to its conflict of laws provisions. Any action or proceeding arising from or relating to this Agreement must be brought in a federal court in the State of New Jersey, and each party irrevocably submits to the jurisdiction and venue of any such court in any such action or proceeding. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to this Agreement.

Exhibit A

General Service Level Support Terms

Up-Time and Reliability. Service Provider will use reasonable commercial efforts with the intent that Services will be available and operational to Customer for 99% of all Scheduled Availability Time. “Scheduled Availability Time” shall be defined as twenty-four (24) hours a day, seven (7) days a week, excluding: (i) scheduled maintenance downtime; (ii) maintenance downtime for specific critical Service issues; and (iii) any downtime due to defects caused by Customer, one of its vendors, third party connections, utilities, or caused by other forces beyond the control of Service Provider (such as internet outages or outages with respect to Customer’s network or internet access). Service Provider shall use reasonable efforts to provide advance notice in writing or by email of any scheduled service disruption. In the event of any unexcused downtime, Service Provider will credit the prorated amount to the Customer’s next monthly invoice.

Maintenance. Service Provider will make available to Customer as part of the Services, all generally available enhancements, updates and bug fixes to the Services.

Customer Responsibility. In addition to other responsibilities contained herein, Customer will be responsible for ongoing maintenance, management and accuracy of the vendor profile data. Additionally, Customer will be responsible for communicating and managing the vendor registration, vendor training and change management process.

Support. Service Provider is available to receive product support inquiries via email or the Service Provider website 24 hours per day. Service Provider Standard Support Hours are 08:30 to 17:30 Eastern Standard Time Monday through Friday for technical information, technical advice and technical consultation regarding Customer’s use of the Services.

Customer Support List. Customer shall provide to Service Provider, and keep current, a list of designated contacts and contact information (the “Support List”) for Service Provider to contact for support services. Such Support List shall include (i) the first person to contact for the answer or assistance desired, and (ii) the persons in successively more responsible or qualified positions to provide the answer or assistance desired.

Classification of Problems. Service Provider shall classify each problem encountered by Customer according to the following definitions and will use reasonable commercial efforts to address the problem in accordance with such classification according to the table below.

SEVERITY LEVELS AND RESPONSE TIMES

Priority code

Priority description

Action required

Expected response times

Guaranteed Response

Times

P1

Mission Critical. Data collection services and data reporting services are down, causing critical impact to business operations; no workaround available.

Escalation in accordance with provisions in “Escalation procedures” section below.

Cymon AI will provide a status update by telephone and/or e-mail within one (1) business hour within the initial occurrence of the P1 issue. Cymon AI ’s goal for resolution of P1 issues is within one (1) calendar day of Customer’s receipt of issue notification.

Cymon AI will provide a status update by telephone and/or e-mail within four (4) business hours within the initial occurrence of the P1 issue.

P2

High. Data collection services and data reporting services are significantly degraded and/or impacting significant aspects of business operations.

Escalation in accordance with provisions in “Escalation procedures” section below.

Cymon AI will provide a status update by telephone, e-mail, or via automated notification within the reporting interface of the Measurement Services as mutually agreed upon by the Parties, as warranted until (i) the problem is resolved, (ii) an acceptable workaround is found or (iii) the problem is determined to be outside of Cymon AI’s ability to control.

Cymon AI will provide a status update by eight (8) business hours within the initial occurrence of the P2 issue.

ESCALATION PROCEDURES

Priority Code	Contact Type	Name of Cymon AI contact/Role	Contact Email address	Time delay before Escalation to next level
P1	Primary	Key Tech Staffer/First Available	support@cymon.ai	2 hours
P1	Secondary	Dedicated Account Manager	support@cymon.ai	4 hours
P2	Primary	All Staff/First Available	support@cymon.ai	8 hours
P2				

Secondary

Dedicated Account Manager

support@cymon.ai

12 hours

Exhibit B

Data Protection Addendum

This Data Protection Addendum ("Addendum") supplements and amends the current version of the agreement between _____ and any of its affiliates (together, "Customer"), and Cymon AI Data, Inc. ("Service Provider"), each a "Party" and collectively the "Parties". This Addendum applies to and takes precedence over the License & Master Services Agreement dated _____ by and between Service Provider and Customer (collectively, the "Agreement"). To the extent of any conflict between the Agreement and the terms of this Addendum, this Addendum shall govern.

Service Provider agrees as follows:

Definitions. For purposes of this Addendum:
"Data Privacy Laws" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, communications secrecy, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("CCPA") and the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR").

"Data Subject" means an identified or identifiable natural person about whom Personal Data relates.

"Personal Data" means data that identifies and individual or is reasonably capable of being associated with an identified individual or device and includes "personal data," "personal information," and "personally identifiable information," and such terms shall have the same meaning as defined by the applicable Data Privacy Laws.

"Process" and "Processing" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

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

"Standard Contractual Clauses" means the annex found in EU Commission Decision of 4 June 2021 on 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, completed as described in the "Data Transfers" section below.

“Subcontractor” means any entity that Service Provider utilizes to fulfill any part of the Agreement with Customer.

Scope and Purposes of Processing.

Service Provider will only Process Personal Data as set forth in this Addendum and in compliance with Data Privacy Laws.

Service Provider will Process all Customer data, including Personal Data, solely to fulfill its obligations to Customer under the Agreement, including this Addendum, and on Customer’s behalf, and for no other purposes, unless required to do otherwise by Data Privacy Laws to which Service Provider is subject. In such case, Service Provider will inform Customer of that legal requirement before such Processing, unless that law prohibits Service Provider from providing such information.

Without limiting the foregoing, Customer directs Service Provider to Process Personal Data in accordance with Customer’s written instructions, as may be provided by Customer to Service Provider from time to time, and in the following manner.

Subject matter, nature, and purpose of Processing: Service Provider will process data solely to fulfill its purposes under the Agreement, which may include any lawful processing or business purposes as provided for under applicable Data Privacy Laws. See the Agreement and Service Provider Researcher Requirements (if applicable) for details.

Anticipated duration of Processing: For the term of the Agreement or to the extent that Service Provider continues to Process Personal Data, whichever is longer.

Categories of Personal Data typically subject to Processing under the Agreement: Personal Data may include, but is not limited to, contact information, date of birth, and employment history.

Typical categories of Data Subjects: Data Subjects could include candidates, customers, prospects, or employees as applicable.

Service Provider will immediately inform Customer if, in Service Provider’s reasonable opinion, an instruction from Customer infringes Data Privacy Laws.

Service Provider will not:

Sell Personal Data.
Process Personal Data for any purpose other than for the specific purposes set forth herein. For the avoidance of doubt, Service Provider will not Process Personal Data outside of the direct business relationship between Customer and Service Provider.

Attempt to link, identify, or otherwise create a relationship between Personal Data and non-Personal Data or any other data without the express authorization of Customer.

Information that has been de-identified is not Personal Data.

Personal Data Processing Requirements. Service Provider will:

Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Upon written request of Customer, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their representatives) for exercising their rights under Data Privacy Laws (such as rights to access or delete Personal Data).

Promptly, and in any event within five days, notify Customer of (i) any third-party or Data Subject requests or complaints regarding the Processing of Personal Data; or (ii) any government or Data Subject requests for access to or information about Service Provider's Processing of Personal Data on Customer's behalf, unless prohibited by Data Privacy Laws. If Service Provider receives a third-party, Data Subject, or governmental request, Service Provider will await written instructions from Customer on how, if at all, to assist in responding to the request. Service Provider will provide Customer with reasonable cooperation and assistance in relation to any such request.

Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data.

Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Service Provider under Data Privacy Laws to consult with a regulatory authority in relation to Service Provider's Processing or proposed Processing of Personal Data.

Data Security. Service Provider will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Exhibit C.
Security Breach. Service Provider will notify Customer promptly, and in any event within forty-eight (48) hours, of any Security Breach. Service Provider will comply with the Security Breach-related obligations directly applicable to it under Data Privacy Laws and will assist Customer in Customer's compliance with its Security Breach-related obligations, including without limitation, by:
At Service Provider's own expense, taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and
Providing Customer with the following information, to the extent known:

The nature of the Security Breach, including, where possible, what happened, the categories and appCymon AIimate number of Data Subjects concerned, and the categories and appCymon AIimate number of Personal Data records concerned;
The likely consequences of the Security Breach; and
Measures taken or proposed to be taken by Service Provider to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.
Service Provider agrees that it will not communicate with any third party, including the media, nor identify Customer in connection with any Security Breach involving Customer data or Customer Personal Data without the express prior written consent and direction of Customer, except and solely to the extent required by law. Notwithstanding the foregoing, Service Provider shall provide Customer with reasonable notice prior to any public announcement of a Security Breach regardless of Customer being named or any impact to Customer data.

Subcontractors.
Customer acknowledges and agrees that Service Provider may use Service Provider affiliates and other Subcontractors to Process Personal Data in accordance with the provisions within this Addendum and Data Privacy Laws. Service Provider shall provide Customer with a current list of subcontractors upon Customer's request.

Where Service Provider sub-contracts any of its rights or obligations concerning Personal Data, including to any affiliate, Service Provider will (i) take steps to select and retain Subcontractors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with Data Privacy Laws; and (ii) enter into a written agreement with each Subcontractor that imposes obligations on the Subcontractor that are no less restrictive than those imposed on Service Provider under this Addendum.

Service Provider will maintain an up-to-date list of its Subcontractors, which it will provide to Customer with reasonable advance notice of any new Subcontractor being able to Process Personal Data. In the event Customer objects to a new Subcontractor, Service Provider will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to Customer's use of the services to avoid Processing of Personal Data by the objected-to Subcontractor without unreasonably burdening Customer. Customer may, in its sole discretion, terminate the Agreement at any time and without prior notice in the event that it objects to a new Subcontractor and Service Provider is unable to change the services to satisfy Customer.

Data Transfers. Service Provider agrees to be bound by the Standard Contractual Clauses to the extent that Service Provider Processes Personal Data of Data Subjects located in the European Economic Area ("EEA"). In case of conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses will prevail. Following Brexit, the relevant terms shall be deemed amended as necessary to legitimize transfers of Personal Data of Data Subjects located in the United Kingdom to and from the United Kingdom and subsequent onward transfers. The Standard Contractual Clauses shall not apply with respect to

Personal Data that Service Provider Processes in the EEA or in a country that the European Commission has decided provides adequate protection for Personal Data.

Audits. Upon request, Service Provider will make available to Customer all information necessary to demonstrate compliance with this Addendum and will allow for and contribute to, no more than once per year (unless there is a Security Breach), audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Return or Destruction of Personal Data. Except to the extent required otherwise by Data Privacy Laws, Service Provider will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer or (b) termination of the Agreement. Except to the extent prohibited by Data Privacy Laws, Service Provider will inform Customer if it is not able to return or delete the Personal Data.

Indemnification. Service Provider will indemnify, defend, and hold harmless Customer and its directors, officers, employees, agents, successors, and permitted assigns (the “Customer Indemnitees”) from and against any losses, claims, damages, demands, liabilities, actions, and related expenses (including reasonable attorneys’ fees) incurred by the Customer Indemnitees arising out of or resulting from third-party claims related to Service Provider’s breach of this Addendum or Data Privacy Laws. The foregoing shall be subject to the limitations of liability provisions in the Agreement.

Term. This Addendum is effective as the effective date of the Agreement.

Survival. The provisions of this Addendum survive the termination or expiration of the Agreement for so long as Service Provider or its Subcontractors Process the Personal Data.

EXHIBIT C

SERVICE PROVIDER DATA SECURITY MEASURES

Service Provider will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Service Provider has agreed to employ appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data ("Information Security Program").

Service Provider's Information Security Program includes specific security requirements for its personnel and all Subcontractors or agents who have access to Customer Personal Data ("Data Personnel").

Service Provider's security requirements cover the following areas:

Information Security Policies and Standards. Service Provider will maintain information security policies, standards and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Customer Personal Data. These policies, standards, and procedures shall be designed and implemented to:

Prevent unauthorized persons from gaining physical access to Customer Personal Data Processing systems (e.g. physical access controls); Prevent Customer Personal Data Processing systems from being used without authorization (e.g. logical access control); Ensure that Data Personnel gain access only to such Customer Personal Data as they are entitled to access (e.g. in accordance with their access rights) and that, in the course of Processing or use and after storage, Customer Personal Data cannot be read, copied, modified or deleted without authorization (e.g. data access controls); Ensure that Customer Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of Customer Personal Data by means of data transmission facilities can be established and verified (e.g. data transfer controls); and Ensure that all systems that Process Customer Personal Data are the subject of a vulnerability management program that includes without limitation internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities. Physical Security. Service Provider will maintain commercially reasonable security systems at all Service Provider sites at which an information system that uses or stores Customer Personal Data is located ("Processing Locations") and will reasonably restrict access to such Processing Locations. Organizational Security. Service Provider will maintain information security policies and procedures addressing: Data Disposal. Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any Customer Personal Data stored on media before they are withdrawn from the Service Provider's inventory or control.

Data Minimization. Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of Customer Personal Data stored on media.

Data Classification. Policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for all employees have been implemented and are maintained.

Incident Response. All Customer Personal Data security incidents are managed in accordance with appropriate incident response procedures.

Network Security. Service Provider maintains commercially reasonable information security policies and procedures addressing network security.
Access Control (Governance).

Service Provider governs access to information systems that Process Customer Personal Data. Only authorized Service Provider staff can grant, modify or revoke access to an information system that Processes Customer Personal Data.

Service Provider implements commercially reasonable physical and technical safeguards to create and protect passwords.

Virus and Malware Controls. Service Provider protects Customer Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Customer Personal Data.

Personnel.
Service Provider has implemented and maintains a security awareness program to train all employees about their security obligations. This program includes training about data classification obligations, physical security controls, security practices, and security incident reporting.

Data Personnel strictly follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.
Service Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may Process Customer Personal Data.

Business Continuity. Service Provider implements disaster recovery and business resumption plans. Business continuity plans are tested and updated regularly to ensure that they are up to date and effective.

Last updated: September 9, 2025