DATA PROCESSING ADDENDUM

Last Updated: October 6, 2026

This Data Processing Addendum (this "DPA") is published by Patra Corporation ("Patra") and applies to Patra's Processing of Personal Data on behalf of each client ("Client") under a Master Services Agreement or other written or online agreement with Patra (the "Agreement"). This DPA applies whether or not the Agreement expressly incorporates it: where the Agreement incorporates this DPA by reference, this DPA forms part of the Agreement on that basis; and where the Agreement does not expressly incorporate this DPA or otherwise address the Processing of Personal Data, this DPA is deemed incorporated into and forms an integral part of the Agreement, governs Patra's Processing of Personal Data thereunder, and supersedes any prior or conflicting data processing terms between the parties. This DPA supplements the Agreement with respect to the Processing of Personal Data by Patra on behalf of Client. In the event of a conflict between this DPA and the Agreement or any other addendum thereto, the order of precedence set forth in Section 15.1 shall apply. All capitalized terms not defined herein have the meanings ascribed in the Agreement.

1. DEFINITIONS

As used in this DPA, the following terms have the meanings set forth below:

"Applicable Data Protection Laws" means all applicable federal, state, and local privacy, data protection, and information security statutes, regulations, rules, and binding guidance in effect during the Term, including without limitation: the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA/CPRA"); the Colorado Privacy Act; the Connecticut Data Privacy Act; the Virginia Consumer Data Protection Act; the Texas Data Privacy and Security Act; the Nevada Privacy of Information Collected on the Internet from Consumers Act; the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations, including the FTC Safeguards Rule; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, where applicable; and any successor legislation or regulations thereto, as each may be amended from time to time.

"Authorized Contact" means a representative of Client designated in writing to provide Processing instructions to Patra under this DPA. Absent any such designation, "Authorized Contact" means the Primary Contact as set forth in the Agreement.

"Aggregated Data" means data that has been combined and summarized at a group or category level such that it cannot reasonably be linked to any identified or identifiable natural person, household, device, or Client.

"Client Information" has the meaning ascribed to it in the Agreement.

"De-Identified Data" means Client Information that has been de-identified in accordance with Section 12 such that it cannot reasonably be used to identify, infer information about, or otherwise be linked to any identified or identifiable natural person, household, device, or Client, provided that Patra: (a) has implemented technical and organizational safeguards that prohibit re-identification of the information; (b) has implemented business processes that specifically prohibit re-identification of the information and that are designed to prevent its inadvertent release in a manner that could permit re-identification; (c) to the extent required by Applicable Data Protection Laws, publicly commits to maintain and use the information only in de-identified form and to not attempt to re-identify it; and (d) contractually obligates any recipient of the information, including

Subprocessors, to comply with each of the foregoing. Patra does not retain any key, crosswalk, or other means capable of relinking De-Identified Data to an identified or identifiable natural person, household, device, or Client.

"Personal Data" or "Personal Information" has the meaning ascribed to such terms under Applicable Data Protection Laws, including "nonpublic personal information" as defined under GLBA and "protected health information" as defined under HIPAA, in each case to the extent applicable to the Services.

"Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, including but not limited to the collection, receipt, access, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure to authorized Subprocessors, transmission, dissemination, combination, restriction, erasure, or deletion of Personal Data as necessary to perform the Services.

"Security Incident" means any confirmed or reasonably suspected unauthorized access to, use, disclosure, alteration, or destruction of Personal Data in Patra's possession or control. An error by Patra's AI Systems in performing the Services within Client Systems in a Client-Side Deployment (each as defined in the AI Addendum), within the access Client has authorized, is not a Security Incident unless it results in unauthorized access to or disclosure of Personal Data, and is otherwise addressed under the Agreement.

"Subprocessor" means any third party engaged by Patra to Process Personal Data on behalf of Client in connection with the Services.

2. ROLES; SCOPE; PROCESSING INSTRUCTIONS

2.1 Roles.

Client, in its capacity as a controller or business under Applicable Data Protection Laws, determines the purposes and means of Processing Personal Data. Patra, in its capacity as a processor or service provider under Applicable Data Protection Laws, Processes Personal Data solely on behalf of and at the direction of Client in accordance with this DPA and the Agreement. Nothing in this DPA shall be construed to render Patra a controller or co-controller with respect to Client's Personal Data.

2.2 Documented Instructions.

Patra shall Process Personal Data only pursuant to documented instructions from Client, including as set forth in the Agreement, any addendum or Statement of Work issued thereunder, a Workflow (as defined in the applicable SOW), this DPA, a written data protection assessment approval, or written communication from an Authorized Contact. Patra shall not Process Personal Data for any purpose not authorized by Client, except as required by Applicable Data Protection Laws.

2.3 Conflicting Instructions.

In the event Patra reasonably determines that any Processing instruction from Client would require Patra to act in violation of Applicable Data Protection Laws, Patra shall notify Client in writing without undue delay. Patra shall be under no obligation to follow such an instruction pending written resolution by the parties, unless otherwise required by law.

2.4 Client Warranties; Notices and Consents.

Client represents and warrants that: (a) Client has provided all notices required by Applicable Data Protection Laws to individuals whose Personal Data is included in Client Information; (b) to the extent that a legal basis beyond notice is required (including, without limitation, consent for

sensitive data categories), Client has obtained and shall maintain all such consents, has implemented and shall honor all applicable opt-in and opt-out signals, and shall ensure the timely recognition of consent withdrawals; (c) all instructions provided by Client to Patra are within Client's lawful authority and are consistent with Client's applicable privacy notices and legal bases for Processing; and (d) Client shall promptly notify Patra in writing if any notice, consent, or lawful basis relevant to Processing is withdrawn, materially changed, or invalidated, and shall cooperate with Patra in implementing any resulting Processing restrictions.

3. SECURITY

3.1 Technical and Organizational Measures.

Patra shall implement and maintain appropriate technical and organizational measures ("TOMs") designed to protect the confidentiality, integrity, and availability of Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Such TOMs shall include, at a minimum: (a) encryption of Personal Data in transit and at rest; (b) access controls, including role-based access, multi-factor authentication, and least-privilege principles; (c) secure software development and change management practices; (d) regular security testing and vulnerability assessments; (e) comprehensive logging and monitoring; and (f) business continuity and disaster recovery plans with defined recovery objectives.

3.2 Personnel Obligations.

Patra shall ensure that all personnel with access to Personal Data are subject to binding confidentiality obligations and receive appropriate privacy and security training commensurate with their role. Access to Personal Data shall be restricted to personnel who require such access to perform the Services.

4. SUBPROCESSORS

Patra may engage Subprocessors to assist in the performance of the Services. Any Subprocessor engaged by Patra shall be bound by written contractual obligations imposing data protection requirements substantially equivalent to those set forth in this DPA, including purpose limitation, confidentiality, security, and data deletion or return obligations. Patra shall remain liable to Client for the acts and omissions of its Subprocessors to the same extent as if Patra had performed such activities directly. Patra will make available to Client, upon request or through a designated online location, a current list of Subprocessors. Third-party providers of artificial intelligence models and cloud infrastructure used to deliver AI-enabled Services may be engaged as Subprocessors and are subject to this Section.

Patra will provide Client with notice of any new Subprocessor that Processes Personal Data, by email to Client's designated contact or by updating the online Subprocessor list, prior to or promptly following the Subprocessor's engagement. If Client reasonably objects to a new Subprocessor on data-protection grounds, the parties will discuss Client's concerns in good faith; if the parties are unable to resolve the objection, Client's sole and exclusive remedy is to terminate the affected Services on written notice. Given the pace of change in AI infrastructure, Client waives any longer advance-notice or prior-approval requirement with respect to AI and cloud Subprocessors.

5. DATA SUBJECT AND CONSUMER RIGHTS

Patra shall provide commercially reasonable cooperation and assistance to Client in responding to verified data subject and consumer rights requests under Applicable Data Protection Laws (including rights of access, correction, deletion, portability, and opt-out of sale/sharing), taking into account the nature of Patra's Processing and the information available to Patra. Patra shall promptly forward to Client, and in any event within ten (10) business days of receipt, any data subject or consumer rights request received directly by Patra that relate to Client's Personal Data. Patra shall not respond to such requests directly without Client's prior written authorization unless required by Applicable Data Protection Laws.

6. PATRA'S ASSISTANCE OBLIGATIONS

Taking into account the nature of Processing and the information available to Patra, Patra shall provide reasonable assistance to Client in ensuring compliance with Client's obligations under Applicable Data Protection Laws, including with respect to: (a) security of Processing; (b) notification of Security Incidents to supervisory authorities and affected individuals; (c) data protection impact assessments; (d) prior consultation with supervisory authorities where required; and (e) responding to data subject and consumer rights requests. Such assistance shall be provided at Client's reasonable written request and at Client's cost where such assistance goes beyond Patra's standard obligations under this DPA.

7. AUDITS; REPORTS; TRANSPARENCY

Upon not less than thirty (30) days' prior written notice from Client, Patra shall make available to Client relevant audit reports and third-party certifications, including, as applicable, SOC 2 Type II reports and ISO 27001 certifications. Client may, at its own cost and no more than once per calendar year (absent a confirmed Security Incident), conduct or commission an audit of Patra's data processing practices relevant to this DPA, subject to reasonable advance notice and Patra's standard audit conditions. Any third-party auditor engaged by Client shall be subject to a confidentiality obligation acceptable to Patra.

8. INTERNATIONAL TRANSFERS

To the extent that Patra Processes Personal Data subject to cross-border transfer restrictions under Applicable Data Protection Laws, the parties shall implement appropriate transfer mechanisms as required, including Standard Contractual Clauses, International Data Transfer Agreements, or equivalent instruments, prior to any such transfer. Patra shall route Processing consistent with any regional processing commitments set forth in the Agreement and shall disclose any exceptions to Client for written approval prior to implementation. The parties acknowledge that Patra's provision of AI-enabled Services may involve Processing in jurisdictions where Patra's model or cloud infrastructure is hosted, and the transfer mechanisms described in this Section shall extend to any such AI-related data flows.

9. RETENTION; RETURN AND DELETION

Patra shall retain Personal Data only for so long as is necessary to perform the Services and as otherwise required by Applicable Data Protection Laws, applicable regulatory obligations, or legitimate security or audit requirements. Upon expiration or termination of the Agreement, or upon Client's written request, Patra shall use commercially reasonable efforts to securely delete or return all identifiable Personal Data in Patra's possession or control, in accordance with Client's

written instructions, unless continued retention is required by any of the foregoing. Patra shall complete such deletion or return within a reasonable period following the applicable trigger, taking into account the volume and nature of the Personal Data and the technical means available to Patra.

10. SECURITY INCIDENTS

10.1 Notification.

Patra shall notify Client without undue delay of Patra's confirmation of a Security Incident involving Personal Data. Such notice shall include, to the extent then known: (a) a description of the nature of the Security Incident, including the categories and approximate volume of Personal Data and data subjects affected; (b) the likely consequences of the Security Incident; (c) the measures Patra has taken or proposes to take to address the Security Incident and mitigate its effects; and (d) the name and contact details of Patra's designated privacy contact. Where full information is not available at the time of the initial notification, Patra shall provide a preliminary notice and supplement it as additional information becomes available.

10.2 Cooperation.

Patra shall cooperate with Client's reasonable requests in connection with the investigation, remediation, and notification obligations arising from a Security Incident. Patra shall not make any public disclosure regarding a Security Incident that identifies or could reasonably be expected to identify Client without Client's prior written consent, except as required by Applicable Data Protection Laws.

11. PURPOSE LIMITATION; NO SALE OR SHARING

Patra shall not: (a) retain, use, or disclose Personal Data for any purpose other than the limited and specified business purposes set forth in the Agreement, any addendum or Statement of Work issued thereunder, a Workflow, and this DPA; (b) sell or share Personal Data as those terms are defined under Applicable Data Protection Laws; or (c) use Personal Data for independent advertising, marketing, or any commercial purpose unrelated to the Services. If Applicable Data Protection Laws require Patra to disclose Personal Data for a purpose unrelated to the business purposes specified herein, Patra shall, unless legally prohibited from doing so, first inform Client of the legal requirement and provide Client a reasonable opportunity to object to or challenge the requirement.

12. DATA MINIMIZATION; DE-IDENTIFICATION

Patra shall implement data minimization practices and adopt appropriate technical and organizational measures designed to limit Personal Data Processing to what is necessary for the performance of the Services. Patra may create De-Identified Data or Aggregated Data from Client Information, and may use, retain, and disclose such De-Identified Data or Aggregated Data for its own research, development, and service-improvement purposes, and shall maintain such data in de-identified form, with no attempt to re-identify. Patra shall, by written contractual obligation, require all relevant Subprocessors to comply with equivalent no re-identification obligations. Patra shall de-identify Client Information using technical and organizational measures that (i) satisfy the de-identification standard under the Applicable Data Protection Laws governing the relevant data; and (ii) are otherwise commercially reasonable and consistent with generally recognized industry standards for de-identification. Data de-identified in accordance with this Section 12 does not constitute Personal Data subject to Applicable Data Protection Laws for so long as Patra continues

to satisfy the safeguards and commitments set forth in clauses (a) through (d) of the definition of "De-Identified Data." If any such data becomes reasonably capable of being linked to an identified or identifiable natural person, household, device, or Client, it shall again be treated as Personal Data under this DPA.

13. RECORDS; DOCUMENTATION

Patra shall maintain records and documentation sufficient to support compliance with this DPA and applicable regulatory requirements, including, as applicable: records of Processing activities; data protection impact assessments; security incident logs; Subprocessor agreements; and change logs.

14. CCPA/CPRA SERVICE PROVIDER MODULE

The following provisions apply to Patra's Processing of Personal Information subject to the CCPA/CPRA in its capacity as a service provider:

(i) Processing of Personal Information under this DPA constitutes a limited and specified business purpose for which Patra is authorized to act as a service provider under the CCPA/CPRA.

(ii) Patra is prohibited from retaining, using, or disclosing Personal Information for any purpose other than the business purposes expressly specified in the Agreement and this DPA, or as otherwise permitted by the CCPA/CPRA and its implementing regulations.

(iii) Patra shall not sell or share Personal Information as those terms are defined under the CCPA/CPRA.

(iv) Patra may create and use De-Identified Data or Aggregated Data, subject to its no re-identification obligations under Section 12.

(v) Patra shall flow down equivalent service provider obligations to all Subprocessors engaged in the Processing of Personal Information subject to the CCPA/CPRA.

(vi) Patra certifies that it understands the restrictions set forth in this Section 14 and the CCPA/CPRA, including the prohibitions on selling or sharing Personal Information and on retaining, using, or disclosing Personal Information outside the permissions set forth in the Agreement and this DPA between the parties, and Patra shall comply with them.

(vii) Where the business purposes require Patra to collect Personal Information from individuals on Client's behalf, Patra shall provide a CCPA/CPRA-compliant notice at collection at Client's direction, using only a notice that Client provides or has approved in writing, and shall not modify or alter such notice without Client's prior written consent.

15. MISCELLANEOUS

15.1. This DPA supplements, and does not limit, Patra's obligations set forth in the Agreement, the Data Security Addendum, and the AI Addendum. In the event of any conflict between this DPA and the Agreement, an SOW, the AI Addendum, or the Data Security Addendum, the following order of precedence shall govern solely to the extent of the conflict: (a) the AI Addendum, with respect to AI-specific Processing, including AI-specific Processing of Personal Data; (b) this DPA, with respect to the Processing of Personal Data; (c) the Data Security Addendum, with respect to information security controls; (d) the applicable SOW, with respect to the scope and performance of the Services; and (e) the Agreement, in all other respects; provided that terms agreed in an SOW or other written agreement for a specific

Client-Side Deployment (as defined in the AI Addendum) shall govern that Client-Side Deployment.

15.2. This DPA shall remain in effect for the duration of the Agreement and shall automatically terminate upon the termination or expiration of the Agreement, subject to any post-termination obligations expressly set forth herein (including Patra's obligations under Section 9 with respect to deletion or return of Personal Data).

15.3. Each party's liability under or in connection with this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement. The parties acknowledge that Applicable Data Protection Laws may impose liability that cannot be contractually excluded or limited, and nothing in this DPA shall be construed to limit either party's liability to the extent such limitation would be prohibited by Applicable Data Protection Laws.

ANNEX A — DETAILS OF PROCESSING

The following schedule describes the details of Patra's Processing of Personal Data under this DPA.

Nature of Processing	Collection, storage, use, disclosure, and deletion of Personal Data as necessary to perform the Services under the Agreement, including insurance back-office operations, document management, policy checking, certificate issuance, and related administrative functions, whether performed on Patra's platform or through Patra's AI Systems operating within Client Systems in a Client-Side Deployment (each as defined in the AI Addendum).
Purpose of Processing	Performance of the Services as described in the Agreement and any applicable Statements of Work; compliance with applicable legal obligations; and the research, development, and service-improvement purposes described in Section 12. Authorized AI-related Processing under the AI Addendum, including model training, fine-tuning, inference, output generation, and Development Activities (as defined in the AI Addendum), is included within these purposes.
Types of Personal Data	May include: policyholder names, addresses, contact information, insurance policy details, certificate holder information, limited professional/commercial identifiers, and, where applicable to the SOW, other categories of Personal Data, potentially including sensitive personal data.
Categories of Data Subjects	Clients' commercial insurance policyholders, certificate holders, and other individuals whose Personal Data is contained in Client Information processed in connection with the Services.
Duration of Processing	For the Term of the Agreement and for such period thereafter as is necessary to fulfill Patra's obligations under Section 9 of this DPA, including any period required by Applicable Data Protection Laws, applicable regulatory obligations, or legitimate security or audit requirements. Personal Data will be deleted or returned in accordance with Section 9 upon expiration of the applicable retention need.
Sub-Processors	Available upon request.