Exhibit C — Data Processing Addendum

Series 2026 | Effective September 2026

Exhibit C - Data Processing Addendum
This Data Processing Addendum (“DPA”) forms part of, and is subject to, the Revomo SaaS Subscription Agreement (the “Agreement”) between Revomo, LLC (“Licensor”) and the entity identified in the applicable Order Form (“Subscriber”). This DPA applies to the extent Licensor Processes Personal Data on behalf of Subscriber in connection with the Service. Capitalized terms used but not defined in this DPA have the meanings given in the Agreement.

1. Definitions

1.1 “Applicable Data Protection Laws” means all data protection and privacy laws and regulations applicable to the Processing of Personal Data under this DPA, including (i) Regulation (EU) 2016/679 (“GDPR”); (ii) the GDPR as incorporated into United Kingdom law (“UK GDPR”); (iii) the Swiss Federal Act on Data Protection (“Swiss FADP”); (iv) the California Consumer Privacy Act, as amended by the CPRA (“CCPA”); and (v) any successor or comparable laws, in each case as amended, supplemented, or replaced.

1.2 “Personal Data” means any information protected as “personal data,” “personal information,” “personally identifiable information,” or a comparable term under Applicable Data Protection Laws that is contained within Subscriber Data.

1.3 “Process” and “Processing” have the meanings given in the GDPR (or, for US Personal Data, the CCPA).

1.4 “Controller,” “Processor,” “Data Subject,” “Business,” “Service Provider,” and “Sell” have the meanings given to them under Applicable Data Protection Laws.

1.5 “Restricted Transfer” means a transfer of Personal Data to a country that is not subject to an adequacy decision under the GDPR, UK GDPR, or Swiss FADP, as applicable.

1.6 “Security Incident” means a confirmed breach of Licensor’s security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to Personal Data Processed by Licensor. Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, or denial-of-service attacks.

1.7 “Standard Contractual Clauses” or “SCCs” means (i) for transfers subject to the GDPR, the clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (“EU SCCs”); and (ii) for transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner’s Office (“UK Addendum”).

1.8 “Subprocessor” means any third party engaged by Licensor (or its affiliates) to Process Personal Data on behalf of Subscriber.

2. Roles of the Parties

For Personal Data subject to the GDPR, UK GDPR, or Swiss FADP, Subscriber is the Controller (or Processor acting on behalf of a third-party Controller) and Licensor is the Processor. For Personal Data subject to the CCPA, Subscriber is the Business and Licensor is a Service Provider. Subscriber is responsible for the legality of the Personal Data it provides and the instructions it issues to Licensor.

3. Scope and Instructions for Processing

3.1 Scope. Licensor will Process Personal Data only (i) on Subscriber’s documented instructions, including as set out in the Agreement, this DPA, and any Order Form; (ii) as necessary to provide, support, secure, and improve the Service; and (iii) as required by applicable law, in which case Licensor will inform Subscriber of the legal requirement before Processing unless prohibited by law.

3.2 CCPA Service Provider Restrictions. Licensor will not (i) Sell or Share Personal Data; (ii) retain, use, or disclose Personal Data outside the direct business relationship between Licensor and Subscriber; (iii) retain,

use, or disclose Personal Data for any purpose other than the business purposes specified in the Agreement; or (iv) combine Personal Data received from Subscriber with personal information received from or on behalf of another person, except as permitted by 11 CCR § 7050(b) for performing a business purpose. Licensor certifies that it understands the foregoing restrictions and will comply with them.

3.3 Aggregated and De-identified Data. Subscriber agrees that Licensor may create and use Aggregated Data (as defined in the Agreement) to operate, support, secure and improve the Service; to develop new products, services, features and analytics; to produce anonymized industry benchmarks and research; to train and improve models; and for marketing. Aggregated Data will be processed only in a form that does not identify, and cannot reasonably be used to identify, Subscriber, any Authorized User, any Data Subject, or any individual customer, transaction, or price. Licensor will not attempt to re-identify Aggregated Data, will not disclose Aggregated Data in any form that reveals Subscriber's identity or Subscriber's confidential pricing, and will maintain commercially reasonable measures to keep such data de-identified. Aggregated Data that meets the foregoing standard does not constitute Personal Data under this DPA.

4. Confidentiality

Licensor will ensure that personnel authorized to Process Personal Data are subject to written confidentiality obligations (or are bound by appropriate statutory obligations of confidentiality) and have received appropriate training on their data protection responsibilities.

5. Security Measures

5.1 Security Program. Licensor will implement and maintain the technical and organizational measures described in Annex 2 and will not materially decrease the overall security of the Service during the Term.

5.2 Audits and Certifications. Licensor maintains independent third-party attestations of its security program (currently a SOC 2 Type II report covering Security, Availability, and Confidentiality). Once per calendar year, Licensor will make a current copy of such report available to Subscriber upon written request and subject to Subscriber’s confidentiality obligations. Such reports satisfy Licensor’s audit obligations under Article 28(3)(h) of the GDPR. To the extent Applicable Data Protection Laws or a competent supervisory authority requires further audit rights, the Parties will cooperate in good faith to scope such audit to minimize disruption and protect the confidentiality and security of Licensor’s other customers.

6. Subprocessors

6.1 General Authorization. Subscriber provides general authorization for Licensor to engage Subprocessors to Process Personal Data in connection with the Service. The current list of authorized Subprocessors is set out in Annex 3.

6.2 Subprocessor Obligations. Licensor will impose on each Subprocessor data protection obligations no less protective than those set out in this DPA, including obligations sufficient to satisfy Article 28(4) of the GDPR. Licensor will remain liable to Subscriber for the performance of each Subprocessor’s obligations.

6.3 Notice and Objection. Licensor will provide Subscriber with at least thirty (30) days’ prior written notice (which may be provided by email or by updating a public list referenced from Licensor’s documentation) before engaging a new Subprocessor. Subscriber may object on reasonable data protection grounds by providing written notice within the notice period. The Parties will work together in good faith to address the objection; if the Parties cannot reach a resolution, Subscriber’s sole remedy is to terminate the affected portion of the Service for which the Subprocessor would be engaged, on written notice to Licensor, with a pro-rata refund of prepaid Fees for the unused portion of the affected Service.

7. Data Subject Rights

Taking into account the nature of the Processing, Licensor will provide reasonable assistance to Subscriber, by appropriate technical and organizational measures and in so far as possible, to enable Subscriber to respond to requests by Data Subjects to exercise their rights under Applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, objection, and not to be subject to automated

decision-making). If a Data Subject submits a request directly to Licensor, Licensor will promptly inform the Data Subject to contact Subscriber and, where required by law, forward the request to Subscriber.

8. Security Incident Notification

Licensor will notify Subscriber without undue delay after confirming a Security Incident. Such notice will include the information reasonably available to Licensor at the time, including a description of the nature of the Security Incident, the categories and approximate number of Data Subjects and records affected (if known), the likely consequences, and the measures taken or proposed to address the Security Incident and mitigate its effects. Licensor will supplement its notice as additional information becomes available. Licensor's notification of, or response to, a Security Incident is not an acknowledgment of fault or liability.

9. International Data Transfers

9.1 Transfer Mechanisms. Where a Restricted Transfer of Personal Data from Subscriber (as data exporter) to Licensor (as data importer) occurs, the Parties agree that the transfer is made subject to the SCCs as set out in this Section 9.

9.2 EU SCCs. For Personal Data subject to the GDPR, Module Two (Controller-to-Processor) of the EU SCCs applies and is incorporated by reference. The Parties agree that: (i) Clause 7 (docking clause) applies; (ii) under Clause 9(a), Option 2 (general written authorization) applies and the notice period in Section 6.3 of this DPA applies; (iii) under Clause 11, the optional independent dispute resolution body language does not apply; (iv) under Clause 17, Option 1 applies and the SCCs are governed by the law of Ireland; (v) under Clause 18(b), disputes are resolved before the courts of Ireland; and (vi) Annexes I, II, and III of the EU SCCs are deemed populated with the information set out in Annexes 1, 2, and 3 of this DPA.

9.3 UK Transfers. For Personal Data subject to the UK GDPR, the UK Addendum applies to the EU SCCs implemented under Section 9.2, with Tables 1–3 of the UK Addendum populated using the information in this DPA and its Annexes, and Table 4 indicating that neither party may end the UK Addendum as set out in Section 19 of the UK Addendum.

9.4 Swiss Transfers. For Personal Data subject to the Swiss FADP, the EU SCCs implemented under Section 9.2 apply with the following adjustments: (i) references to the GDPR are interpreted as references to the Swiss FADP; (ii) references to “EU,” “Union,” or “Member State law” are interpreted as references to Switzerland or Swiss law; (iii) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and (iv) the SCCs protect the data of legal entities until the revised FADP applies.

10. Return or Deletion of Personal Data

Within thirty (30) days following expiration or termination of the Agreement, Subscriber may request in writing a copy of its then-current Personal Data in a commercially reasonable format. After the expiration of such thirty (30)-day period, Licensor may delete Personal Data from its active systems in the ordinary course, subject to applicable backup retention schedules, legal hold obligations, and the retention permitted under Section 3.3 for Aggregated Data. Backup copies will be deleted in accordance with Licensor’s standard retention cycles and will remain subject to the confidentiality and security obligations of this DPA until deletion.

11. General

11.1 Order of Precedence. In the event of any conflict or inconsistency among the following documents, the order of precedence is: (i) the SCCs (where applicable to a Restricted Transfer); (ii) this DPA; (iii) the Agreement; and (iv) any Order Form. Except as expressly modified by this DPA, the Agreement remains in full force and effect.

11.2 Changes in Law. If a change in Applicable Data Protection Laws requires modification of this DPA, the Parties will negotiate in good faith to amend this DPA within a reasonable time. If the Parties cannot agree on the necessary modifications, Licensor may, on written notice to Subscriber, suspend the affected Processing or terminate the affected portion of the Service without penalty.

11.3 Liability. Each Party's liability under this DPA is subject to the limitations of liability set out in the Agreement. For the avoidance of doubt, the liability cap and exclusions in the Agreement apply to all claims, in aggregate, arising under both the Agreement and this DPA.

11.4 Survival. This DPA terminates simultaneously and automatically with the Agreement. Provisions that by their nature are intended to survive (including obligations relating to confidentiality, security, return or deletion of Personal Data, and any Processing that continues after termination) will survive termination or expiration of the Agreement and this DPA until Licensor has returned or deleted all Personal Data in accordance with this DPA.

11.5 Governing Law. This DPA is governed by the law and jurisdiction provisions of the Agreement, except where Applicable Data Protection Laws or the SCCs require otherwise.

11.6 Severability. If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions will continue in full force and effect.

Annex 1

Description of the Processing

A. List of Parties

Data Exporter	Subscriber, as identified in the Order Form. Acting as Controller (or Processor on behalf of a third-party Controller).
Data Importer	Revomo, LLC, 27 Andrew Ln, Hawthorn Woods, IL 60047, USA. Acting as Processor (Service Provider under the CCPA).

B. Description of the Transfer

Categories of Data Subjects	Subscriber's personnel and authorized users of the Service; Subscriber's customers, prospects, and other business contacts whose identifying information appears in transactional or pricing data that Subscriber uploads to or generates within the Service.
Categories of Personal Data	Business contact information (name, business email, business phone, job title, employer); account credentials and authentication data for the Service; usage and log data (IP address, device identifiers, session timestamps); customer/account identifiers appearing in transactional records uploaded by Subscriber.
Sensitive or Special Category Data	None. The Service is not intended to Process sensitive or special category data. Subscriber agrees not to upload such data without Licensor's prior written consent and any additional safeguards required by Applicable Data Protection Laws.
Frequency of Transfer	Continuous, for the duration of the Term.
Nature and Purpose of Processing	Hosting, storage, retrieval, display, transmission, and other operations reasonably necessary to provide, support, secure, and improve the Service in accordance with the Agreement; technical support; and disclosures required by law.
Duration of Processing	For the Term of the Agreement and any post-termination period during which Licensor continues to hold Personal Data, until return or deletion under Section 10 of this DPA.

Subprocessors	See Annex 3. Duration of Processing by each Subprocessor matches the Term.

C. Competent Supervisory Authority

For transfers subject to the GDPR, the supervisory authority is determined under Clause 13 of the EU SCCs. For transfers subject to the UK GDPR, the UK Information Commissioner's Office. For transfers subject to the Swiss FADP, the Swiss Federal Data Protection and Information Commissioner.

Annex 2

Technical and Organizational Security Measures

Licensor maintains a documented information security program designed to protect the confidentiality, integrity, and availability of Personal Data. Licensor's program is attested under SOC 2 Type II for the Security, Availability, and Confidentiality trust service criteria, and is continuously monitored using Sprinto. The program includes the measures described below.

1. Organizational Security
    - Written information security policies reviewed at least annually and approved by management.
    - Designated personnel responsible for information security and data protection.
    - Mandatory security and privacy awareness training for all personnel at hire and at least annually.
    - Background checks for personnel with access to Personal Data, to the extent permitted by law.
    - Written confidentiality obligations binding on all personnel.
2. Access Controls
    - Role-based access controls enforcing the principle of least privilege.
    - Multi-factor authentication required for administrative access to production systems.
    - Centralized identity management and single sign-on for internal systems.
    - Quarterly access reviews; prompt revocation of access on role change or termination.
    - Unique user identifiers; shared credentials are prohibited for production access.
3. Encryption
    - Personal Data encrypted in transit using TLS 1.2 or higher.
    - Personal Data encrypted at rest using AES-256 or equivalent.
    - Cryptographic keys managed through a dedicated key management service with restricted access.
4. Infrastructure and Network Security
    - Production environment hosted on Amazon Web Services in a multi-availability-zone configuration.
    - Logical network segmentation; production isolated from non-production environments.
    - Web application firewall and intrusion detection on production ingress.
    - Hardened operating system baselines; automated patching of supported components.
    - Centralized logging and monitoring of security-relevant events.
5. Application Security
    - Secure software development lifecycle with peer code review prior to merge.
    - Static analysis and dependency vulnerability scanning in the build pipeline.
    - Annual third-party penetration testing of the Service; identified findings remediated based on risk.
    - Separation of development, staging, and production environments.
6. Business Continuity and Resilience
    - Automated backups of production data with periodic restore testing.
    - Documented disaster recovery and business continuity plans; reviewed at least annually.
    - Multi-availability-zone architecture supporting high availability.
7. Incident Response
    - Documented incident response plan with defined roles, escalation paths, and response timelines.
    - 24/7 monitoring of production environments for security events.
    - Post-incident reviews to identify root causes and improvements.
    - Notification of confirmed Security Incidents in accordance with Section 8 of this DPA.
8. Vendor and Subprocessor Management
    - Security and privacy due diligence for Subprocessors that Process Personal Data.

- Written contracts requiring data protection commitments are no less protective than this DPA.
- Periodic review of Subprocessor security posture and certifications.

9. Audits and Attestations

- SOC 2 Type II report covering Security, Availability, and Confidentiality, refreshed annually.
- Continuous compliance monitoring via Sprinto.
- Subscriber may request the current SOC 2 report as set out in Section 5.2 of this DPA.

Annex 3

Authorized Subprocessors

The Subscriber authorizes the Subprocessors listed below to Process Personal Data in connection with the Service. Licensor will provide notice of any addition or replacement in accordance with Section 6.3 of this DPA.

Subprocessor	Purpose	Location of Processing	Safeguards
Amazon Web Services, Inc.	Hosting and infrastructure (ECS, Batch, Lambda, ElastiCache/Redis, Cognito, S3, ECR, CloudWatch, Secrets Manager, KMS); AI model inference via Amazon Bedrock	United States	SOC 1/2/3, ISO 27001, AWS DPA, EU SCCs as applicable.
MongoDB, Inc.	Application database (Atlas, hosted in AWS)	United States	Provider DPA; EU SCCs as applicable.
ClickHouse, Inc.	Analytical data store for pricing and margin analytics	United States	Provider DPA; EU SCCs as applicable.
Gleap GmbH	In-product support and user feedback	Austria	Provider DPA; EU SCCs as applicable.

Signatures

By signing below, each Party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them.

Subscriber By: Name: Title: Date:	Revomo, LLC By: Name: Title: Date: