# DATA PROCESSING ADDENDUM

This Data Protection Addendum ("**Addendum**") forms part of the Terms of Service or other written agreement, as agreed to by the parties, (collectively, the "**Agreement**") between the customer that has accepted the Terms of Service expressly incorporating this Addendum or has entered into a mutually executed written agreement incorporating this Addendum **(**"**Customer**"**)**, and Alchemy Technologies Incorporated (d/b/a Replo) ("**Processor**"). Customer and Processor are each referred to as a **"Party"** and collectively as the **"Parties**". Any terms used but not defined herein shall have the meaning as set forth in the Agreement.

Except as modified below, the terms of the Agreement shall remain in full force and effect. Notwithstanding anything to the contrary in the Agreement, if there is a conflict between this Addendum and the Agreement, this Addendum will control. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

**1. Definitions**. The terms used in this Addendum shall have the meanings set forth in this Addendum or as defined by Applicable Privacy Law, whichever is broader. Capitalized terms not otherwise defined herein or defined by Applicable Privacy Law shall have the meaning given to them in the Agreement. The following terms have the meanings set forth below:

**1.1 "*Affiliate*"** means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with either Processor or Customer, respectively.

**1.2** "***Applicable Privacy Law***" shall mean applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which Processor is subject, including, but not limited to, (a) the California Consumer Privacy Act of 2018 ("***CCPA***"), (b) the EU General Data Protection Regulation 2016/679 ("***GDPR***") including the applicable implementing legislation of each Member State ("***EU GDPR***"), (c) the UK Data Protection Act 2018 and the UK General Data Protection Regulation as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("***UK GDPR***" and together with the EU GDPR, the "***GDPR***"), (d) the Swiss Federal Act on Data Protection of 19 June 1992, (e) any other applicable law with respect to any Personal Data in respect of which the Processor is subject to, and (f) any other data protection law and any guidance or statutory codes of practice issued by any relevant Privacy Authority, in each case, as amended from time to time and any successor legislation to the same.

**1.3** "***Data Subject***" shall mean an identified or identifiable natural person.

**1.4** "***EEA***" means the European Economic Area.

**1.5** "***Personal Data***" shall mean (i) personal data, personal information, personally identifiable information, or similar term as defined by Applicable Privacy law or (ii) if not defined by Applicable Privacy Law, any information that relates to a Data Subject; in each case, to the extent Processed by Processor, on behalf of Customer, in connection with Processor's performance of the Services.

**1.6 *"Processor Entity"*** shall mean Processor and/or any Processor Affiliate.

**1.7** "***Privacy Authority***" shall mean any competent supervisory authority, attorney general, or other regulator with responsibility for privacy or data protection matters in the jurisdiction of Processor.

**1.8 *"Process", "Processing" or "Processed"*** shall mean any operation or set of operations, as defined in the Applicable Privacy Law, performed upon Personal Data whether or not by automatic means, including collecting, recording, organising, storing, adapting or altering, retrieving,

consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data.

**1.9** "***Security Breach***" means a breach of Processor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Processor's possession, custody or control. Security Breaches do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

**1.10** "***Services***" shall mean the services as described in the Agreement or any related order form or statement of work.

**1.11** "***Standard Contractual Clauses***" means (a) with respect to restricted transfers (as such term is defined under Applicable Privacy Law) which are subject to the EU GDPR and other Applicable Privacy Laws pursuant to which the same have been adopted, the Controller-to-Processor standard contractual clauses, as set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR, as may be amended or replaced by the European Commission from time to time (the "***EU SCCs***"), and (b) with respect to restricted transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual of 21 March 2022, as may be amended or replaced by the UK Information Commissioner's Office from time to time (the "***UK SCCs***").

**1.12** "***Subprocessor***" shall mean any subcontractor (including any third party and/or Processor Affiliate) engaged by Processor to Process Personal Data on behalf of Customer.

**1.13** "***Supervisory Authority***" shall mean: (a) in the context of the UK GDPR the UK Information Commissioner's Office; and (b) in the context of the EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

**2. Processing Requirements**.

**2.1** Processor shall comply with Applicable Privacy Law in the Processing of Personal Data and only Process Personal Data for the purposes of providing the Services and in accordance with Customer's instructions, and as may subsequently be agreed between the Parties in writing. Processor shall promptly inform Customer if (a) in Processor's opinion, an instruction from Customer violates Applicable Privacy Law; or (b) Processor is required by applicable law to otherwise Process Personal Data, unless Processor is prohibited by that law from notifying Customer under applicable law.

**2.2** Processor shall implement and maintain reasonable and appropriate technical measures that will ensure that Customer's reasonable and lawful instructions can be complied with, including the following:

(a) updating, amending, correcting, or providing access to the Personal Data of any Data Subject upon written request of Customer from time to time;

(b) cancelling, deleting, or blocking access to any Personal Data upon receipt of written instructions from Customer;

(c) otherwise facilitating Customer's responses to Data Subject requests as required under Applicable Privacy Law; and

(d) Processor shall promptly re-direct any request from a Data Subject to exercise any of its Data Subject rights to Customer and shall not respond directly to the Data Subject unless instructed so by Customer in writing.

**2.3** Processor acknowledges that (a) Customer discloses Personal Data to Processor solely for the business purpose of Customer, and (b) Processor has not and will not receive any monetary or other valuable consideration in exchange for their receipt of the Personal Data, and that any consideration paid by Customer to Processor under the Agreement relates only to Processor's provision of the Services. Processor shall not collect, retain, use, disclose, or otherwise Process the Personal Data (i) for any purpose other than for the specific purpose of providing the Services to Customer, or (ii) outside of the direct business relationship between Processor and Customer. In addition, Processor shall not 'sell,' as defined under Applicable Privacy Law (including, without limitation, CCPA), or otherwise disclose any Personal Data except to authorised Subprocessors needed to render the Services.

**2.4** Processor shall provide to Customer such co-operation, assistance and information as Customer may reasonably request to enable it to comply with its obligations under Applicable Privacy Law and co-operate and comply with the directions or decisions of a relevant Privacy Authority, in each case (a) solely to the extent applicable to Customer's provision of the Services, and (b) within such reasonable time as would enable Customer to meet any time limit imposed by the Privacy Authority.

**3. Security of Personal Data**.

**3.1** Processor shall maintain, during the term of the Agreement, appropriate technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, as set forth in Exhibit B.

**3.2** Processor shall ensure the reliability of any employees who Process Personal Data.

**4. Customer Obligations**. Customer is solely responsible for its use of the Services, including (a) obtaining any needed consents or authorizations for Processor to Process Personal Data; (b) without limitation of Processor's obligations under Section 3 (Security of Personal Data), making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (c) securing the account authentication credentials, systems and devices Customer uses to access the Services; (d) securing Customer's systems and devices that Processor uses to provide the Services; and (e) backing up Personal Data.

**5. Subprocessors**.

**5.1** Customer generally authorizes Processor to engage Subprocessors to Process Personal Data on Customer's behalf, including the Subprocessors specified in Exhibit C. Processor shall maintain a current list of Subprocessors at replo.app/subprocessors. Processor shall give Customer written notice by email of any intended addition or replacement at least 15 calendar days before the Subprocessor begins Processing Customer's Personal Data, or earlier where necessary to provide a reasonable opportunity to object under Applicable Privacy Law or the Standard Contractual Clauses. Notice shall identify the Subprocessor, its processing activities, and provide information reasonably necessary to assess the change. Notice shall be sent to Customer's designated subprocessor-notice contact or, if none, its account administrator. Customer may designate or update that contact through the notification subscription mechanism. Customer may object on reasonable data-protection grounds by emailing privacy@replo.app within the notice period. Failure to object following that notice constitutes authorization of the notified change. Failure to subscribe does not waive Customer's notice or objection rights.

**5.2** Processor shall remain liable for any Processing of Personal Data by each such Subprocessor as if it had undertaken such Processing itself.

**5.3** Processor will contractually impose data protection obligations on its Subprocessors that are no less onerous than those imposed on Processor under this Addendum.

**6. Breach Notification**.

**6.1 Notification to Customer**. Unless otherwise prohibited by applicable law, Processor shall notify Customer without undue delay, and in any event within 72 hours after Processor becomes aware of a Security Breach. Such notification shall include, to the extent such information is available (a) a detailed description of the Security Breach, (b) the type of data that was the subject of the Security Breach and (c) the identity of each affected person (or, where not possible, the approximate number of Data Subjects and of Personal Data records concerned). In addition, Processor shall communicate to Customer (i) the name and contact details of Processor's data protection officer or other point of contact where more information can be obtained, (ii) a description of the likely consequences of the Security Breach, (iii) a description of the measures taken or proposed to be taken by Processor to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

**6.2 Investigation.** Processor shall take prompt action to investigate the Security Breach and shall use industry standard, commercially reasonable efforts to mitigate the effects of any such Security Breach in accordance with its obligations hereunder.

**7. Privacy Impact Assessment**. Processor shall, promptly upon receipt of written request by Customer (a) make available to Customer such information as is reasonably necessary to demonstrate Customer's compliance with Applicable Privacy Law to the extent applicable to the Services, and (b) reasonably assist Customer in carrying out any privacy impact assessment and any required prior consultations with Privacy Authorities, taking into account the nature of the Processing and the information available to Processor. Processor shall reasonably cooperate with Customer to implement such mitigation actions as are reasonably required to address privacy risks identified in any such privacy impact assessment. Unless such request follows a Security Breach or is otherwise required by Applicable Privacy Law, Customer shall not make any such request more than once in any 12-month period.

**8. Audit Rights**. Customer may audit Processor's compliance with its obligations under this Addendum up to once per year and on such other occasions as may be required by Applicable Data Privacy Laws, including where mandated by Customer's Supervisory Authority. Processor will contribute to such audits by providing Customer or Customer's Supervisory Authority with the information and assistance that Processor considers appropriate in the circumstances and reasonably necessary to conduct the audit. To request an audit, Customer must submit a proposed audit plan to Processor at least two weeks in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Processor will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Processor security, privacy, employment or other relevant policies). Processor will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 8 shall require Processor to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Processor has confirmed there have been no known material changes in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Processor's safety, security or other relevant policies, and may not unreasonably interfere with Processor business activities. Any audits are at Customer's sole expense. Customer shall reimburse Processor for any time expended by Processor and any third parties in connection with any audits or inspections under this Section 8 at Processor's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

**9. Deletion of Personal Data**. Upon expiration or termination of the Agreement, the end of the relevant Services, or receipt of a written deletion instruction from Customer, Processor shall delete and procure the deletion of the affected Personal Data Processed on Customer's behalf, including all

copies, promptly and in any event within 90 days after the applicable event, unless an earlier deadline is required by Applicable Privacy Law. The 90-day outside limit does not extend any shorter deletion deadline promised in Processor's Privacy Policy. Customer shall have a reasonable opportunity to elect return before deletion. If Customer elects return, Processor shall first return a complete copy of the affected Personal Data by secure file transfer in a format reasonably specified by Customer and then delete remaining copies within the foregoing deadline. Otherwise, Processor shall delete by default without a separate deletion request. Cancellation or nonpayment of a paid subscription does not by itself end authorized free Services that Customer continues to receive under the Agreement and this Addendum. Continued Processing is permitted only to the extent and for as long as necessary for those ongoing Services, subject to Customer's deletion instructions, Applicable Privacy Law, the Standard Contractual Clauses and applicable Google requirements. Where law requires retention, Processor shall retain only the minimum required Personal Data, protect it under this Addendum, use it only for that legal requirement and delete it when the requirement ends.

**10. Third Party Disclosure Requests**.

**10.1** Unless prohibited by applicable law, Processor shall promptly notify Customer of any inquiry, communication, request or complaint, to the extent relating to Processor's Processing of Personal Data on behalf of Customer, from:

(a) any governmental, regulatory or supervisory authority, including Privacy Authorities or the U.S. Federal Trade Commission; and/or

(b) any Data Subject,

and shall, taking into account the nature of the Processing, provide reasonable assistance to enable Customer to respond to such inquiries, communications, requests or complaints and to meet applicable statutory or regulatory deadlines. Processor shall not disclose Personal Data to any of the persons or entities in (a) or (b) above unless it is legally required to do so and has otherwise complied with the obligations in this Section 10.1 and Section 10.2.

**10.2** In the event that Processor is required by law, court order, warrant, or other legal judicial process ("***Legal Request***") to disclose any Personal Data to any person or entity other than Customer, including any national security authority or other government body, Processor shall attempt to redirect the government request to Customer. If Processor is unable to redirect the request, Processor shall, unless prohibited by applicable law, notify Customer promptly and shall provide all reasonable assistance to Customer to enable Customer to respond or object to, or challenge, any such Legal Requests and to meet applicable statutory or regulatory deadlines. If Processor is prohibited by applicable law from providing notice to Customer of a Legal Request, Processor shall use commercially reasonable efforts to object to, or challenge, any such Legal Request to avoid or minimize the disclosure of Personal Data. Processor shall not disclose Personal Data pursuant to a Legal Request unless it is required to do so by applicable law and has otherwise complied with the obligations in this Section 10.2.

**11. Transfers out of the EEA**. If Customer transfers Personal Data out of the EEA to Processor in a country not deemed by the European Commission to have adequate data protection, such transfer will be governed by the EU SCCs, the terms of which are hereby incorporated into this Addendum. Processor shall provide a copy of the signed version of the EU SCCs to Customer upon request. In furtherance of the foregoing, the parties agree that:

**11.1** Customer will act as the data exporter and Processor will act as the data importer under the EU SCCs;

**11.2** for purposes of Appendix 1 to the EU SCCs, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Section B to Exhibit A;

**11.3** for purposes of Appendix 2 to the EU SCCs, the technical and organizational measures shall be as set out in Exhibit B;

**11.4** the audits described in Clause 8.9 of the EU SCCs shall be performed in accordance with Section 8 of this Addendum;

**11.5** Customer's authorizations in Section 5 (Subprocessors) of this Addendum will constitute Customer's general written authorization to the subcontracting by Processor of the Processing of Personal Data under Clause 9(a)(Option 2) of the EU SCCs. The advance notice period in Section 5.1 applies for purposes of that clause;

**11.6** the Supervisory Authority for the EU SCCs shall be satisfied by the information in Section C of Exhibit A.

**11.7** Option 1 of Clause 17 shall apply, and the EU SCCs will be governed by the law of Ireland; and

**11.8** any dispute arising from the EU SCCs shall be resolved by the courts of Ireland.

**12. Transfers out of the UK**. If Customer transfers Personal Data out of the UK to Processor in a country not deemed by the UK Government to have adequate data protection, such transfer will be governed by the UK SCCs, the terms of which are hereby incorporated into this Addendum. Processor shall provide a copy of the signed version of the UK SCCs to Customer upon request. In furtherance of the foregoing, the parties agree that Tables 1 through 4 of the UK SCCs shall be satisfied by the following information:

**12.1** Table 1: Reference to Table 1 shall be satisfied by the information in Section A of Exhibit A.

**12.2** Table 2: For Table 2, the version of the Approved EU SCCs shall be the EU SCCs, Controller to Processor module.

**12.3** Table 3: Reference to Table 3 shall be satisfied by the information in Exhibit A.

**12.4** Table 4: For Table 4, the Exporter and Importer shall have the rights outlined in Section 19 of the UK SCCs.

**13. Claims**. Any claims brought under, or in connection with, this Addendum, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

This Addendum is binding on Processor and Customer upon Customer's acceptance of the Terms of Service expressly incorporating it by reference, or upon mutual execution of a separate written agreement incorporating it. No separate signature of this Addendum is required for acceptance through the Terms of Service.

**EXHIBIT A**

## A. LIST OF PARTIES

**Data exporter(s):**

| | |
|---|---|
| **Name:** | Customer identified in the applicable Account or order records |
| **Address:** | Customer's address in the applicable Account or order records |
| **Contact person's name, position and contact details:** | Customer's designated contact in the applicable Account or order records |
| **Activities relevant to the data transferred under these Clauses:** | Customer's use of the Services under the Agreement |
| **Signature:** | Acceptance of this Addendum and the incorporated Standard Contractual Clauses through the Terms of Service acceptance record or mutually executed agreement |
| **Date:** | Date of acceptance recorded in the applicable acceptance record or mutually executed agreement |
| **Role (Controller or Processor):** | Controller |

**Data importer(s):**

| | |
|---|---|
| **Name:** | Alchemy Technologies Incorporated (d/b/a Replo) |
| **Address:** | 800 Market Street, Suite 600, San Francisco, CA 94103, USA |
| **Contact person's name, position and contact details:** | Yuxin Zhu, CEO, privacy@replo.app |
| **Activities relevant to the data transferred under these Clauses:** | Processor's provision of the Services under the Agreement |
| **Signature:** | Acceptance of this Addendum and the incorporated Standard Contractual Clauses through the Terms of Service acceptance record or mutually executed agreement |

| | |
|---|---|
| **Date:** | Date of acceptance recorded in the applicable acceptance record or mutually executed agreement |
| **Role (Controller or Processor):** | Processor |

## B. DESCRIPTION OF TRANSFER

| | |
|---|---|
| **Categories of data subjects whose personal data is transferred** | Registered users (businesses and individuals with Processor accounts, including workspace members); visitors to Processor customers' storefronts or websites where Processor's analytics script is deployed; employees, officers, and representatives of Customer and its affiliates. |
| **Categories of personal data transferred** | Name, email address, billing/shipping address, payment method type, account credentials, usage and engagement data, browsing activity on Customer-operated pages (e.g., pages visited, time on page, scroll depth, click interactions), order line-item details, campaign/ad performance data, photos and videos uploaded by users, and any other personal data Customer provides to Processor in connection with the Services. |
| **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures** | Sensitive data is not anticipated in the ordinary course of the Services. Processor does not knowingly collect biometric, health, or financial account number data. To the extent any sensitive data is incidentally processed it will be subject to the same technical and organizational safeguards as other Personal Data. |
| **The frequency of the transfer (whether the data is transferred on a one-off or continuous basis)** | On a continuous basis during the term of the Agreement. |
| **Nature of the processing** | As described in the Agreement. |

| | |
|---|---|
| **Purpose(s) of the data transfer and further processing** | As described in the Agreement. |
| **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period** | Duration of the relevant Services, subject to the return, deletion and limited retention provisions in Section 9 of this Addendum. |
| **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing** | As described in the Agreement. |

## C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be the supervisory authority that has jurisdiction over the Data Exporter/Controller.

## EXHIBIT B

## TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

*Processor has implemented and will maintain the following technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, in accordance with Article 32 GDPR and applicable data protection laws. Processor may update these measures from time to time, provided that the overall level of security is not materially diminished.*

**1. Access Controls.** Role-based access on a least-privilege, need-to-know basis; unique user credentials; access to production systems restricted to authorized personnel only; prompt revocation of access upon personnel departure or role change.

**2. Encryption in Transit.** All data transmitted between users and Processor's services is encrypted in transit using industry-standard TLS/HTTPS protocols.

**3. Encryption at Rest.** Encryption at rest is handled by Processor's infrastructure subprocessors (primarily AWS and Heroku); Processor does not manage server-level encryption directly. Sensitive credentials (e.g., Shopify API keys) are separately encrypted within Processor's database. Passwords are hashed using industry-standard hashing practices.

**4. Confidentiality.** All personnel and contractors with access to Personal Data are bound by written confidentiality obligations.

**5. Network and System Security.** Processor uses standard TLS/HTTPS for all communications. Operating systems and software are kept reasonably up to date. Access to production systems is logged where available.

**6. Segregation.** Logical separation of Customer data from data of other customers and from Processor's internal environments.

**7. Physical Security.** Processor does not operate dedicated data centers. Primary infrastructure is hosted with AWS and Heroku, which maintain their own physical security controls. Processor offices maintain reasonable physical access controls appropriate to a processional services environment.

**8. Subprocessor Management.** Written agreements with subprocessors imposing data protection obligations no less protective than those in this Addendum; periodic review of material subprocessors.

**9. Incident Response.** Documented security incident response procedures; notification to Customer without undue delay (and in any event within 72 hours) after becoming aware of a Personal Data Breach affecting Customer data.

**10. Personnel**. Access to Personal Data is restricted to authorized personnel on a need-to-know basis. Employees are informed of data protections and security obligations relevant to their roles.

**11. AI/Model Use.** Processor shall not use Customer Personal Data to train, fine-tune, or develop its own or any third party's generative or machine-learning models, except as expressly instructed or permitted by Customer in writing. Processor may use commercially available artificial intelligence tools (including those listed in Exhibit C) as part of its standard operational and development workflow, provided that such tools operate under data processing agreements expressly prohibiting the provider from using inputs for model training or retaining inputs for the provider's own purposes. Notwithstanding the foregoing or any Customer instruction or permission, Processor and its

Subprocessors shall Process Personal Data obtained through Google APIs, and data derived from it, only as permitted by the applicable Google API Services User Data Policy, including applicable Limited Use requirements and Google Workspace and other service-specific restrictions. Neither Processor nor its Subprocessors may use or transfer such data to develop, train, or improve non-personalized artificial intelligence or machine-learning models. Customer's written instruction or permission does not authorize Processing prohibited by those requirements.

**12. Data Return and Deletion.** At the end of the relevant Services, Processor delete Personal Data by default, or return it first if elected by Customer and then delete remaining copies, in accordance with Section 9 of this Addendum, subject to applicable legal retention requirements.

**13. Review.** Processor periodically reviews and assesses the effectiveness of these measures and updates them as appropriate.

## EXHIBIT C

## LIST OF SUB-PROCESSORS

Processor's list of Subprocessors, including their identities and processing activities, is maintained at replo.app/subprocessors and is incorporated herein by reference as Exhibit C. Additions and replacements are subject to the notice and objection requirements in Section 5.1.