Alchemy Data Protection Addendum

Last Updated: June 30, 2023

This Data Protection Addendum (including its Attachments) ("**DPA**") forms part of and is subject to the terms and conditions of the Alchemy Terms of Service (the "**Agreement**") by and between you ("**Company**") and Alchemy Insights, Inc. ("**Alchemy**"), and is binding as of the Effective Date.

1. SUBJECT MATTER AND DURATION.

1.1. **Subject Matter**. This DPA sets forth the terms by which the Parties will comply with Data Protection Laws in connection with the Agreement. All capitalized terms not defined in this DPA will have the meanings given to them in the Agreement. If and to the extent language in this DPA or any of its attachments conflicts with the Agreement, this DPA shall control.

1.2. **Duration and Survival**. This DPA will become legally binding upon the effective date of the Agreement. Alchemy will Process Company Personal Data until termination of the Agreement.

2. DEFINITIONS. For the purposes of this DPA, the following terms and those defined within the body of this DPA apply.

2.1. "**Company Personal Data**" means Your Data that is Personal Data Processed by Alchemy on behalf of Company.

2.2. "**Data Protection Laws**" means the applicable data privacy and data protection laws, rules, and regulations to which Company is subject in relation to Company Personal Data. "**Data Protection Laws**" may include, but are not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).

2.3. "**Personal Data**" has the meaning assigned to the term "**personal data**" or "**personal information**" under applicable Data Protection Laws.

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

2.5. "**Security Incident(s)**" means a breach of Alchemy's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Personal Data.

2.6. "**Subprocessor(s)**" means Alchemy's authorized vendors and third-party service providers that Process Company Personal Data.

3. PROCESSING TERMS FOR COMPANY PERSONAL DATA.

3.1. **Documented Instructions**. Alchemy shall Process Company Personal Data in accordance with the Agreement, this DPA, any applicable Order Form, and any written documented instructions provided by Company and agreed upon by Alchemy. Alchemy will, unless legally prohibited from doing so, inform Company in writing if it reasonably believes that there is a conflict between Company's instructions and any law that is applicable to Company.

3.2. **Authorization to Use Subprocessors**. To the extent necessary to fulfill Alchemy's contractual obligations under the Agreement, Company hereby authorizes Alchemy to engage Subprocessors.

3.3. **Alchemy and Subprocessor Compliance**. Alchemy shall: (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Company Personal Data that imposes on such Subprocessors data protection requirements for Company Personal Data that are consistent with this DPA; and (ii) remain responsible to Company for Alchemy's

Subprocessors' failure to perform their obligations with respect to the Processing of Company Personal Data in accordance with such written agreements.

3.4. **Right to Object to Subprocessors**. Where required by Data Protection Laws, Alchemy will notify Company prior to engaging any new Subprocessors that Process Company Personal Data by updating its Subprocessor list available at [https://www.alchemy.com/policies/dpa/subprocessors] (**"Subprocessor Website"**). The Subprocessor Website also contains a mechanism for Company to subscribe to notifications of any updates and if Company subscribes to such notifications, Alchemy will email Company new Subprocessor notifications at the email address provided. Company will have ten (10) days to object after notice has been provided on Subprocessor Website or via email (as applicable). If Company raises legitimate objections to the appointment of any new Subprocessor, Alchemy will determine whether it can resolve the grounds for the objection and if it is unable to do so within sixty (60) days then Alchemy may terminate the Agreement without penalty.

3.5. **Confidentiality**. Any person authorized to Process Company Personal Data must contractually agree to maintain the confidentiality of such information or be subject to a statutory obligation of confidentiality.

3.6. **Personal Data Inquiries and Requests**. Where required by Data Protection Laws, Alchemy agrees to provide reasonable assistance at Company's expense, and comply with reasonable instructions from Company related to any requests from individuals exercising their rights in Company Personal Data granted to them under Data Protection Laws.

3.7. **Sale of Company Personal Data Prohibited**. Alchemy shall not sell Company Personal Data as the term "sell" is defined by the CCPA.

3.8. **Data Protection Impact Assessment and Prior Consultation**. Where required by Data Protection Laws, Alchemy agrees to provide reasonable assistance at Company's expense to Company where the type of Processing performed by Alchemy requires a data protection impact assessment or prior consultation with the relevant data protection authorities.

3.9. **Demonstrable Compliance**. Alchemy agrees to provide information to demonstrate compliance with this DPA upon Company's reasonable request. 3.10. Service Optimization. Alchemy may Process Company Personal Data: (i) for its internal uses to build or improve the quality of its services; (ii) to detect Security Incidents; and (iii) to protect against fraudulent or illegal activity.

3.10. **Service Optimization**. Alchemy may Process Company Personal Data: (i) for its internal uses to build or improve the quality of its services; (ii) to detect Security Incidents; and (iii) to protect against fraudulent or illegal activity.

4. INFORMATION SECURITY PROGRAM. Alchemy shall implement and maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Company Personal Data.

5. NOTICE OF SECURITY INCIDENTS. Upon becoming aware of a Security Incident, Alchemy agrees to provide written notice to Company without undue delay. Where the Security Incident is caused by Alchemy's intentional or negligent acts or omissions, such notice will include all available details required under Data Protection Laws for Company to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

6. CROSS-BORDER TRANSFERS OF COMPANY PERSONAL DATA.

6.1. Cross-Border Transfers of Company Personal Data. Company authorizes Alchemy and its Subprocessors to transfer Company Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

6.2. EEA, Swiss, and UK Standard Contractual Clauses. If Company Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Company to Alchemy in a country that has not been found to provide an adequate level of protection under applicable Data 2 Protection Laws, the Parties agree that the transfer shall be governed by Module Two's obligations in the Annex to the Commission Implementing Decision (EU) 2021/914 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 (**"Standard Contractual Clauses"**) as supplemented by Attachment 1 attached hereto, the terms of which are incorporated herein by reference. Each Party's execution of the Agreement shall be considered a

signature to the Standard Contractual Clauses and UK Addendum, where required.

7. AUDITS. Where required by Data Protection Laws, Company (or its appointed representative) may carry out an audit of Alchemy' policies, procedures, and records relevant to the Processing of Company Personal Data. Any audit shall be at Company's expense and must be: (i) conducted during Alchemy' regular business hours; (ii) with no less than 30 days' advance notice to Alchemy; (iii) carried out in a manner that prevents unnecessary disruption to Alchemy' operations; (iv) subject to reasonable confidentiality procedures; and (v) conducted no more than once per year, unless carried out at the direction of a government authority having proper jurisdiction.

8. COMPANY PERSONAL DATA DELETION. At the expiry or termination of the Agreement, Alchemy will, upon Company's written request, delete all Company Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Alchemy' data retention schedule), except where Alchemy is required to retain copies under applicable laws, in which case Alchemy will isolate and protect that Company Personal Data from any further Processing except to the extent permitted by applicable laws.

9. PROCESSING DETAILS.

9.1. Subject Matter. The subject matter of the Processing is the Subscription Services pursuant to the Agreement.

9.2. Duration. The Processing will continue until the expiration or termination of the Agreement.

9.3. Categories of Data Subjects. Data subjects whose Company Personal Data will be Processed pursuant to the Agreement.

9.4. Nature and Purpose of the Processing. The nature and purpose of the Processing of Company Personal Data by Alchemy is the performance of the Subscription Services.

9.5. Types of Company Personal Data. Company Personal Data that is Processed pursuant to the Agreement.

ATTACHMENT 1 TO THE DATA PROTECTION ADDENDUM

This Attachment 1 forms part of the DPA and supplements the Standard Contractual Clauses. Capitalized terms not defined in this Attachment 1 have the meaning set forth in the DPA.

The Parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. SUPPLEMENTAL TERMS. The Parties agree that:

(i) a new Clause 1(e) is added to the Standard Contractual Clauses stating: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.";

(ii) a new Clause 1(f) is added to the Standard Contractual Clauses stating: "To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).";

(iii) the optional text in Clause 7 is deleted;

(iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer will inform data exporter of new subprocessors in accordance with Section 3(d) of the DPA;

(v) the optional text in Clause 11 is deleted; and

(vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. ANNEX I. Annex I to the Standard Contractual Clauses shall read as follows:

A. List of Parties

(1) Data Exporter: Company.

Address: As set forth in the Notices section of the Agreement.

Contact person's name, position, and contact details: As set forth in the Notices section of the Agreement.

Activities relevant to the data transferred under these Clauses: The Subscription Services.

Role: Controller.

(2) Data Importer: Alchemy.

Address: As set forth in the Notices section of the Agreement.

Contact person's name, position, and contact details: As set forth in the Notices section of the Agreement.

Activities relevant to the data transferred under these Clauses: The Subscription Services.

Role: Processor.

B. Description of the Transfer:

Categories of data subjects whose personal data is transferred:

Employees, contractors or other personnel of Subscriber, Subscriber's end users, and third-parties whose information is provided by Subscriber or end users.

Categories of personal data transferred:

IP address, wallet addresses, and information stored on a blockchain

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:

To the Parties' knowledge, no sensitive data is transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Personal data is transferred when the Services are used, or as otherwise agreed upon by the Parties.

Nature of the processing:

APIs to facilitate Subscriber's services to end users, including processing of information to be read from or written to a blockchain.

Purpose(s) of the data transfer and further processing:

For the users of the Subscription Services to enjoy the Services whether or not such use is necessary for the purposes of this Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Data importer will retain personal data in accordance with Alchemy's data retention policies. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: To provide APIs to enable Subscribers to read from or write to a blockchain in connection with providing services to Subscriber's end users, and to enable Subscriber's personnel to log into the Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

To provide APIs to enable Subscribers to read from or write to a blockchain in connection with providing services to Subscriber's end users, and to enable Subscriber's personnel to log into the Services.

C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the Parties consistent with the conditions set forth in Clause 13.

D. Additional Data Transfer Impact Assessment Questions:

Will data importer process any personal data under the Clauses about a non-United States person that is "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)?

Not to data importer's knowledge.

Is data importer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where personal data is stored or accessed from that would interfere with data importer fulfilling its obligations under the Clauses? For example, FISA Section 702. If yes, please list these laws:

Data importer does not provide telecommunications services and is not considered an electronic communications service ("ECS") provider, and therefore would not be subject to such interference, including under FISA Section 702.

Has data importer ever received a request from public authorities for information pursuant to the laws contemplated by the question above? If yes, please explain:

No.

Has data importer ever received a request from public authorities for personal data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

No.

E. Data Transfer Impact Assessment Outcome: Taking into account the information and obligations set forth in the DPA and, as may be the case for a Party, such Party's independent research, to the Parties' knowledge, the personal data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the Clauses to a country that has not been found to provide an adequate level of protection under applicable data protection laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable data protection laws.

F. Clarifying Terms: The Parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Clauses shall be carried out in accordance with Section 7 of the DPA; (iv) where permitted by applicable data protection laws, data importer may engage existing subprocessors using European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors and such use of subprocessors shall be deemed to comply with Clause 9 of the Clauses; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Clauses will be limited to the termination of the Clauses; (vi) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Clauses; (vii) the information required under Clause 15.1(c) of the Clauses will be provided upon data exporter's written request; and (viii) notwithstanding anything to the contrary, data exporter will reimburse data importer for all costs and expenses incurred by data importer in connection with the performance of data importer's obligations under Clause 15.1(b) and Clause 15.2 of the Clauses without regard for any limitation of liability set forth in the Agreement.

3. ANNEX II.

Annex II of the Standard Contractual Clauses shall read as follows:

Data importer shall implement and maintain commercially reasonable technical and organizational measures designed to protect personal data in accordance with the DPA.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPA.

4. ANNEX III. A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the DPA. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the DPA.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Clauses.

Table 4: The Parties agree that Importer may end the UK Addendum as set out in Section 19.