APOLLO GRAPH, INC.

DATA PROCESSING ADDENDUM

This Data Processing Addendum with its appendices (together, this "**DPA**") is incorporated into the mutually executed GraphOS Subscription Agreement, or other mutually executed governing agreement, between Apollo and Customer that expressly references this DPA ("**Agreement**"). Unless otherwise defined in this DPA or the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA (DEFINITIONS). This DPA is effective as of the effective date of the Agreement.

1. DEFINITIONS. The following capitalized terms used in this DPA will be defined as follows:

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time.

"**Controller**" means entity determining the purposes and means of Processing Covered Data.

"**Covered Data**" means Personal Data that is provided by or on behalf of Customer to Apollo for the purposes of providing the Offerings, as further described in Appendix A.

"**Covered Data Breach**" means a confirmed or reasonably suspected breach of Apollo's security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Covered Data.

"**Data Subject**" means a natural person whose Personal Data is Processed.

"**Data Subject Request**" means a request from a Data Subject exercising a right under Applicable Data Protection Laws, relating to Covered Data and identifying Customer.

"**EEA**" means the European Economic Area including the European Union ("**EU**").

"**GDPR**" means Regulation (EU) 2016/679 ("**EU GDPR**") or, where applicable, "**UK GDPR**", as defined in section 3 of the UK Data Protection Act 2018.

"**Offerings**" means Apollo's software-as-a-service offerings (under the brand name "**Apollo Studio**" as of the effective date of the DPA under and defined as "**Cloud Products**" in Apollo's GraphOS Subscription Agreement) to be provided by Apollo pursuant to the Order(s) issued under the Agreement.

"**Personal Data**" means any data or information that is: (a) linked or reasonably linkable to an identified or identifiable natural person; or (b) otherwise "**personal data**," "**personal information**," "**personally identifiable information**," or similarly defined data or information under Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means or not. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Processor**" means the entity Processing Personal Data on behalf of a Controller.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for international transfers annexed to the European Commission's implementing decision on standard contractual clauses for personal data transfer to third countries under Regulation (EU) 2016/679, published on June 4, 2021, including as incorporated into the UK Transfer Addendum, if applicable.

"**Swiss Data Protection Laws**" means the Swiss Federal Act Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

"**Sub-processor**" means an entity appointed by Apollo to Process Covered Data on its behalf.

"**UK GDPR**" means the EU GDPR as saved into United Kingdom ("**UK**") law by virtue of section 3 of the UK's European Union (Withdrawal) Act 2018.

"**UK Transfer Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, published by the UK Information Commissioner's Office on March 21, 2022.

"**US Data Protection Laws**" means all applicable federal and state laws rules, regulations, and governmental requirements relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States. To the extent applicable, the US Data Protection Laws include the CCPA as defined in Appendix C.

2. PURPOSE; ROLE OF THE PARTIES. This DPA governs Apollo's Processing of Covered Data when providing Offerings under the Agreement. Both parties acknowledge that: (a) for the purposes of the GDPR and Swiss Data Protection Laws, Apollo acts as a "**processor**" (as defined in the GDPR) in the performance of its obligations under the Agreement and this DPA and Customer acts as a "**controller**" (as defined in the GDPR); and (b) for the purposes of the US Data Protection Laws, Apollo will act as a "**Service Provider**" or "**processor**" (each as defined in US Data Protection Laws), as applicable, in its performance of its obligations under the Agreement and this DPA.

3. DATA PROCESSING

3.1 Details and Compliance. The details of the Processing of Covered Data under the Agreement and this DPA, including subject matter, nature and purpose of the Processing, categories of Personal Data, and Data Subjects, are described in the Agreement and Appendix A. Both parties agree to comply with Applicable Data Protection Laws in fulfilling their obligations under this DPA.

3.2 Apollo Responsibilities. Apollo will process Covered Data in accordance with: (a) this DPA; (b) the Agreement; and (c) Orders issued under the Agreement (collectively, the "**Documented Instructions**"). Additionally, Apollo will: (y) provide Customer with information to enable Customer to conduct and document any data protection assessments required under Applicable Data Protection Laws; and (z) promptly notify Customer if it becomes aware of any conflict between the Documented Instructions and Applicable Data Protection Laws.

3.3 Customer Responsibilities. Customer is responsible for ensuring that no special categories of Personal Data (under GDPR Article 9), Personal Data relating to criminal convictions and offenses (under GDPR Article 10), or similarly sensitive Personal Data (as defined in Applicable Data Protection Laws), including but not limited to health information, biometric data, genetic data, or data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual orientation, are submitted to Apollo for Processing.

3.4 Disclosure Restrictions. Apollo will limit access to Covered Data to personnel who have a business need to access such data. Apollo will ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement, including duties of confidentiality with respect to any Covered Data they access. Apollo will maintain the confidentiality of the Covered Data and, except as set out in Section 6 (SUB-PROCESSORS), will not disclose the Covered Data to third parties unless Customer specifically authorizes the disclosure, or as required by domestic law, court, or regulator. If a domestic law, court, or regulator requires Apollo to Process or disclose the Covered Data to a third party, Apollo must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless applicable laws prohibit giving such notice.

4. TERM. This DPA is effective until either the Agreement expires or is terminated, or all Covered Data has been returned or deleted as specified in Section 8 (DATA DELETION), whichever occurs later.

5. SECURITY. Apollo shall implement and maintain appropriate technical and organizational security measures designed to protect Covered Data from Covered Data Breaches and to preserve the security and confidentiality of the Covered Data in accordance with Apollo's Security Measures (as defined in the Agreement). Apollo may review and update its Security Measures from time to time, provided that any such updates shall not materially diminish the overall security of the Offerings or Covered Data or otherwise amend this DPA or Apollo's obligations pertaining to the Processing of Covered Data. Apollo will implement and maintain, as a minimum standard, the technical and organizational measures described in Appendix B.

6. SUB-PROCESSORS

6.1 Authorized Sub-Processors. Subject to Section 6.2 (Change Notification), Apollo may Process Covered Data anywhere that Apollo or its Sub-processors maintain facilities. Customer generally authorizes the engagement of the Sub-processors listed in Appendix A or as otherwise set forth in the "**Sub-Processor Documentation**" (collectively, the "**Authorized Sub-processors**"). Apollo has entered, or will enter, into a written agreement with each Sub-processor imposing data protection obligations that are, in substance, no less protective of Covered Data than Apollo's obligations under this DPA.

6.2 Change Notification. Apollo will provide Customer with at least 14 days' notice ("**Objection Period**") of any proposed changes to the Authorized Sub-processors. During the Objection Period, Customer may object, on reasonable grounds related to the protection of Covered Data, to the proposed change to the Authorized Sub-processors. This can include exercising its right to object under clause 9(a) of the SCCs, by sending an email to legal@apollographql.com (with a copy to support@apollographql.com) describing its legitimate, good-faith objection. Apollo may address the objection by: (a) not using the new Sub-

processor to Process Covered Data; (b) taking corrective steps requested by Customer; or (c) ceasing to provide the parts of the Offerings that involve the new Sub-processor Processing Covered Data, subject to a mutual agreement of the parties. The parties will work together in good faith to resolve any objections raised by Customer. If Apollo and Customer are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may terminate the portion of the Agreement relating to the Offerings affected by such change by providing written notice to Apollo.

7. DATA SUBJECT REQUESTS. If Apollo receives a Data Subject Request, Apollo will promptly direct the Data Subject to submit their request to Customer and notify Customer of the received request. If Customer is unable to independently address the request or access the Covered Data, then upon Customer's written request, Apollo shall provide commercially reasonable cooperation to assist Customer in responding to any Data Subject Requests. Customer will be responsible for responding to any such Data Subject Request.

8. DATA DELETION. Customer may retrieve or delete all Covered Data either: (a) at any time upon written request to Apollo during the term of the Agreement; or (b) during any post-termination Retrieval Period (as defined in the Agreement) following the expiration or termination of the Agreement. For any Covered Data not deleted by Customer prior to expiration or termination of the Agreement or during any post-termination Retrieval Period, Apollo will initiate a deletion process upon the later of: (y) expiration or termination of the Agreement; or (z) expiration of any post-termination Retrieval Period. Apollo's deletion process will delete Covered Data within 180 days. If Apollo must retain any Covered Data due to legal obligations, this DPA will continue to apply to that Covered Data. Customer is responsible for exporting any data Customer wishes to retain before the deletion process begins.

9. COVERED DATA BREACH. Upon confirming or reasonably suspecting any Covered Data Breach, Apollo will notify Customer in writing without undue delay, and in any case within 72 hours. This notification will include, to the extent known: (a) the nature of the Covered Data Breach; (b) the measures taken to mitigate or contain the Covered Data Breach; and (c) the status of the investigation. If complete information is not immediately available, Apollo will provide updates as soon as possible. Apollo will promptly take all reasonable steps to contain, investigate, and mitigate any Covered Data Breach. Apollo's notification or response to a Covered Data Breach shall not be considered an acknowledgment of fault or liability with respect to the Covered Data Breach. These obligations do not cover breaches caused by the Customer, end-users of the Offerings, or Third-Party Applications (as defined in the Agreement). Should the Customer decide to notify authorities, Data Subjects, or the public about a breach, the Customer will, subject to legal requirements, endeavor to provide Apollo with advance notice and an opportunity for input.

10. CUSTOMER AUDIT RIGHTS. Customer may audit Apollo's compliance with its obligations under this DPA up to once per calendar year, provided that this annual limit does not apply if more frequent audits are required by Applicable Data Protection Laws or if mandated by Customer's supervisory authority. Apollo will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance that Apollo considers appropriate and reasonably necessary to conduct the audit. If a third party is to conduct the audit, Apollo may object if the auditor is, in Apollo's reasonable opinion, not independent or otherwise manifestly unsuitable. Such an objection by Apollo will require Customer to appoint another auditor or conduct the audit itself. If Customer (acting reasonably) provides documentary evidence that the information made available by Apollo is not sufficient to demonstrate Apollo's compliance with this DPA, Apollo shall allow for and contribute to audits by Customer, or a third-party auditor mandated by Customer regarding the processing of Customer Personal Data by Apollo. To request an audit, Customer must submit a proposed audit plan to Apollo at least 30 days in advance of the proposed audit date (except where an audit is mandated by Applicable Data Protection Laws or Customer's supervisory authority, in which case the proposed audit plan must be submitted as soon as practically possible). Any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties, 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 scope, duration, and start date of the audit. Apollo will review the proposed audit plan and provide Customer with any concerns or questions, such as any request for information that could compromise Apollo's security, privacy, employment, or other relevant policies. Apollo will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 10 (CUSTOMER AUDIT RIGHTS) shall require Apollo 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 12 months of Customer's audit request and Apollo 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 Apollo's safety, security, or other relevant policies, and may not unreasonably interfere with Apollo's business activities. Customer shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any damage, injury, or disruption to Apollo's systems, equipment, personnel, data, and business (including any interference with the confidentiality or

security of the data of Apollo's other customers or the availability of Apollo's products and services to such other customers). Customer will promptly notify Apollo of any non-compliance discovered during the course of an audit and provide Apollo with any audit reports generated in connection with any audit under this Section 10 (CUSTOMER AUDIT RIGHTS), unless prohibited by Applicable Data Protection Laws or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA or as required by Applicable Data Protection Laws or its supervisory authority. Any audits are at Customer's sole expense.

11. IMPACT ASSESSMENTS. Apollo will use commercially reasonable efforts to assist Customer in conducting data protection impact assessments by providing necessary documentation and participating in assessments as required. This assistance will consider the nature of the Processing and the information available to Apollo. This obligation applies specifically to matters related to the Offerings and when Customer lacks access to relevant information.

12. DATA TRANSFERS

12.1 Restricted Transfer. The parties acknowledge that transfers of Covered Data to Apollo that are subject to an applicable adequacy decision do not require a separate approved transfer mechanism. If a transfer of Covered Data to Apollo is not subject to an applicable adequacy decision ("**Restricted Transfer**"), the Restricted Transfer is made in accordance with the below.

12.2 Transfers from the EEA. Where a Restricted Transfer is made from the EEA, the SCCs are incorporated into this DPA and apply to the transfer as follows:

(a) Module Two applies where Customer is a Controller and Apollo is a Processor, and Module Three applies where both Customer and Apollo are Processors;

(b) in Clause 7, the optional docking clause does not apply;

(c) in Clause 9(a) of Modules Two and Three, Option 2 applies, and the period for prior notice of Sub-processor changes is set forth in Section 6 of this DPA (SUB-PROCESSORS);

(d) in Clause 11(a), the optional language does not apply;

(e) in Clause 17, Option 1 applies with the governing law being that of Ireland;

(f) in Clause 18(b), disputes will be resolved before the courts in Dublin, Ireland;

(g) Annex I of the SCCs is completed with the information in Appendix A to this DPA;

(h) Annex II of the SCCs is completed with the information in Appendix B to this DPA; and

(i) Annex III of the SCCs is completed with the Sub-processor information listed in Appendix A and the Sub-processor Documentation.

12.3 Transfers from Switzerland. Where a Restricted Transfer is made from Switzerland, the SCCs are incorporated into this DPA and apply to the transfer as modified in Section 12.2 (Transfers from the EEA), except that:

(a) in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner;

(b) references to "**Member State**" in the SCCs refer to Switzerland, and data subjects located in Switzerland may exercise and enforce their rights under the SCCs in Switzerland; and

(c) references to the "**General Data Protection Regulation**," "**Regulation 2016/679**," and "**GDPR**" in the SCCs refer to the Swiss Data Protection Laws.

12.4 Transfers from the UK. Where a Restricted Transfer is made from the United Kingdom, the UK Transfer Addendum is incorporated into this DPA and applies to the transfer. The UK Transfer Addendum is completed with the information in Section 12.2 of this DPA (Transfers from the EEA), the Sub-processors listed in Appendix A and the Sub-processor Documentation, and Appendices A and B to this DPA; and both "**Importer**" and "**Exporter**" are selected in Table 4 of the UK Transfer Addendum.

12.5 Specific application of the SCCs. The following terms apply to the SCCs:

(a) Customer may exercise its audit rights under the SCCs as set out in Section 10 (CUSTOMER AUDIT RIGHTS) above.

(b) Apollo may appoint Sub-processors under the SCCs as set out in Section 6 (SUB-PROCESSORS) above.

(c) With respect to Restricted Transfers made to Apollo, Apollo may neither participate in, nor permit any Sub-processor to participate in, any further Restricted Transfer unless the further Restricted Transfer is made in full compliance with Data Protection Laws and in accordance with applicable SCCs or an alternative legally compliant transfer mechanism.

(d) If any provision of this Section 12 (DATA TRANSFERS) is inconsistent with any terms in the SCCs, the SCCs prevail.

13. LIMITATION OF LIABILITY. The liability of each party for data breaches and non-compliance with this DPA shall be capped at the maximum amount permitted under the Agreement.

14. CONFLICT. In the event of a conflict or inconsistency between the Agreement, this DPA, and the SCCs, the terms of the following documents will prevail (in order of precedence): SCCs, DPA, and Agreement.

15. MODIFICATIONS. Apollo may change this DPA where (a) the change is required to comply with Applicable Data Protection Laws; or (b) the change is commercially reasonable, does not materially reduce the security of the Offerings, does not change the scope of Apollo's processing of Covered Data, and does not have a material adverse impact on Customer's rights under this DPA.

Appendix A to DPA

Details of Processing and Transfers

A. LIST OF PARTIES

Data exporter(s):

Name: Customer

Address: The address for Customer associated with its operative Order or as otherwise stated in the Agreement

Contact person: The contact details for Customer associated with its operative Order or as otherwise stated in the Agreement

Activities relevant to the transfer: Processing Personal Data for the purpose of accessing and receiving the Offerings

Signature and date: The parties agree that execution of the Agreement constitutes execution of this Appendix A by both parties.

Role (controller/processor): Processor or Controller

Data importer(s):

Name: Apollo Graph, Inc.

Address: 1600 Bryant Street, #411447, SMB#20356, San Francisco, CA, 94141 USA

Contact person: The contact details for Apollo as stated in the Agreement. Apollo's legal team and privacy team can be contacted at legal@apollographql.com.

Activities relevant to the transfer: Processing Personal Data for the purpose of providing, supporting, and improving the Offerings

Signature and date: The parties agree that execution of the Agreement constitutes execution of this Appendix A by both parties.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Customer's employees and contractors who are authorized end-users of Offerings or otherwise authorized to receive routine business communications related to the Offerings (e.g., support requests, billing, etc.).

Categories of personal data transferred: "Business Contact Information," such as name, business email address, business title, and IP address

Special category or other sensitive data transferred (if applicable) and applied restrictions or safeguards: N/A (none). No special category or sensitive data is transferred.

Frequency of the transfer: Continuous

Nature of the processing: Collection, storage, deletion, rectification, aggregation as described in the Agreement, Order(s), DPA, and Documentation.

Purpose(s) of the transfer and further processing: For Apollo to provide, support, and improve the Offerings, in particular to enable access and authenticate login events and provide routine business communications (e.g., responding to support requests)

Retention period: If Personal Data is not deleted upon request by Customer during the term of the Agreement, the duration of Processing will be as long as this DPA remains in effect, as more particularly set out in Section 6 of the DPA (DATA DELETION).

Sub-processors: The subject matter of Personal Data transferred to Sub-processors is Business Contact Information, which is transferred to Sub-processors to provide, support, and improve the Offerings, in particular for hosting the Offerings and enabling user management and enabling Apollo to provide routine business communications (e.g., responding to support requests):

Sub-processors involved in providing the Offerings:

- Google Cloud (hosting and analytics), as of the effective date of the DPA, using following data center zones:

    - US-Central 1 – Iowa
    - US-East 1 - South Carolina
    - US-East 4 - (Ashburn) Northern Virginia
    - US-West 1 - Boardman, Oregon
    - US-West 2 - Los Angeles
    - US-West 3 - Salt Lake City
- Amazon Web Services (hosting and analytics), as of the effective date of the DPA, using following data center zones:
    - US East-1 Northern Virginia
    - US East-2 Ohio
    - US West-2 Oregon
    - US West-1 Northern California
- PingOne (user management) located in the United States
- GitHub (optional)* (user management) located in the United States
    - **Authorized end-users of the Offering (i.e., Apollo Studio) have the option of using their existing GitHub account to sign into their Apollo Studio account.*

Additional Sub-processors who do not host or otherwise provide the Offerings but may Process Personal Data on Apollo's behalf in other routine business communication and operation capacities, are listed in the Sub-Processor Documentation set forth in Section 6.1 (Authorized Sub-Processors).

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the supervisory authority of Ireland.

Appendix B to DPA

Technical and Organizational Measures

Apollo has implemented and will maintain the technical and organizational measures set out in the Security Measures referenced in the Agreement. As of the effective date of this DPA, such technical and organizational measures encompass the following:

1. **Access Management**
   - Apollo limits access to Covered Data to personnel with a legitimate business need or role-based requirement for such access.
   - Apollo implements and maintains user access controls that ensure prompt provisioning and deprovisioning of user accounts.

2. **Auditing and Compliance**
   - Throughout the Agreement's duration, Apollo commits to maintaining SSAE 18 SOC 2 certification or an equivalent standard. This certification will undergo annual renewal. Upon Customer request, Apollo will provide a summary of its most recent SOC 2 Type II report once per 12-month period during the Agreement term. In the event Apollo secures additional security certification reports (e.g., ISO 27001), Apollo will provide a summary such report once per 12-month period during the Agreement term.
   - Apollo adheres to guidelines from ISO 27001, NIST, and other industry-recognized best practices.

3. **Operational Continuity**
   - Apollo develops and maintains business continuity, backup, and disaster recovery plans (collectively, "**BC/DR Plans**") to minimize service disruptions and ensure compliance with applicable laws.
   - The BC/DR Plans address potential threats to Offerings and their dependencies and establish procedures for resuming Offerings access and usage.
   - Apollo conducts regular testing of the BC/DR Plans at predetermined intervals.

4. **Change Management**
   - Apollo upholds policies and procedures for implementing changes to Offerings, including underlying infrastructure and system components, to ensure adherence to quality standards.
   - Apollo conducts annual penetration testing of its network and Offerings. Any identified vulnerabilities will be addressed and evaluated in accordance with Apollo's policies and procedures.
   - Apollo performs regular vulnerability scans of its network, assessing and addressing any findings in line with its policies and procedures.
   - Security patches are applied according to Apollo's established patching schedule.
   - Apollo maintains separate environments for testing and development, distinct from the production environment.

5. **Data Protection**
   - Apollo implements technical safeguards and other security measures to ensure the security and confidentiality of Covered Data.
   - Apollo ensures logical segregation of Covered Data within the production environment.

6. **Encryption and Key Management**
   - Apollo maintains policies and procedures for managing encryption mechanisms and cryptographic keys within Apollo's cryptosystem.
   - Apollo employs industry-standard encryption practices for data at rest and in transit across public networks, as applicable.

7. **Governance and Risk Management**
   - Apollo maintains an information security program subject to at least annual review.
   - Apollo conducts a risk management program, including risk assessments performed at minimum annually.

8. **Personnel Security and Training**
   - Apollo engages a third-party to conduct background verifications for all Apollo personnel who have access to Covered Data.
   - Apollo mandates that all employees complete initial (upon hiring) and annual security awareness training.

Appendix C to DPA

CCPA Terms

These CCPA Terms are applicable when the California Consumer Privacy Act of 2018, Cal. Civ. Code §§1798.100–1798.199.100, as amended, and the CCPA regulations, Cal. Code Regs. §§7000–7304 (collectively referred to as the "**CCPA**") apply to Customer's utilization of the Offerings to process Covered Data. For the purposes of these CCPA Terms, the terms "**Commercial Purpose**", "**Consumer**", "**Personal Information**", "**Sell**", "**Service Provider**", and "**Share**" shall have the meanings assigned to them in the CCPA.

Apollo's Obligations. Apollo shall: (a) not Sell or Share Covered Data; (b) process Covered Data solely for the purpose of providing, supporting, and enhancing the Offerings as per the Agreement or Orders, or as otherwise permitted under the CCPA; (c) not retain, use, or disclose Covered Data (i) for any purpose, including any Commercial Purpose, except to provide, support, and improve the Offerings in accordance with the Agreement or Orders, or as otherwise permitted under the CCPA, (ii) outside the direct business relationship between Apollo and Customer, or (iii) in any manner prohibited by the CCPA; (d) not combine Covered Data received from, or on behalf of, Customer with Personal Information received from, or on behalf of, another person or from Apollo's own interactions with the Consumer to whom the Personal Information relates, except to the extent a Service Provider is permitted to do so under the CCPA; (e) comply with all applicable obligations under, and provide the same level of privacy protection to Covered Data as required by, the CCPA; (f) notify Customer if Apollo believes it cannot meet its obligations under the CCPA; and (g) upon Customer's request, and taking into account the nature of the Covered Data processed, provide reasonable assistance to Customer in fulfilling consumer requests made under the CCPA, to the extent Customer is unable to address a particular request on its own through use of the Offerings.

Customer's Obligations and Rights. Customer may: (a) only disclose Covered Data to Apollo for the purpose of using the Offerings in accordance with the Agreement; (b) audit Apollo's compliance with its obligations under this Appendix C by requesting and reviewing: (i) copies of or extracts from Apollo's audit reports related to the security of the Offerings, or (ii) other information Apollo deems reasonably necessary to demonstrate its compliance; and (c) upon notice to Apollo, take reasonable and appropriate steps to halt and rectify any unauthorized use of Covered Data by Apollo.