APOLLO DATA PROCESSING ADDENDUM

This is a reference copy of Apollo's Data Processing Addendum ("**DPA**") and may be required for some Apollo customers. If applicable and mutually executed, this DPA amends the terms and forms part of the Agreement (defined below) by and between the legal entity defined as Customer in the Agreement ("**Customer**") and Apollo Graph, Inc. ("**Apollo**") and shall be effective on the later of (i) the effective date of the Agreement; or (ii) the date both parties execute this DPA ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

Customer's signatory represents to Apollo that they have the legal authority to bind Customer and is lawfully able to enter into this DPA. Notwithstanding the expiration or termination of the Agreement, this DPA and any Standard Contractual Clauses (if applicable) will remain in effect until, and will terminate automatically upon, deletion by Apollo of all Personal Data covered by this DPA. To sign this DPA and receive a countersigned copy, please reach out to your Apollo customer success or sales representative or email legal@apollographql.com.

1. Definitions. For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

"Agreement" means the contract in place between Customer and Apollo and in connection with Customer's subscription to the Services.

"Applicable Data Protection Laws" means US Data Protection Law and EU Data Protection Laws that are applicable to the processing of Customer Personal Data under this DPA.

"controller", "data subject", "personal data", **"processing"** (and **"process"**), **"processor",** and **"supervisory authority"** shall have the meanings given in EU Data Protection Laws. The term "controller" includes "business", the term "data subject" includes "consumers", and the term "processor" includes "service provider" (in each case, as defined by the CCPA).

"Customer Data" shall have the meaning described in the Agreement. To the extent not defined in the Agreement, Customer Data shall mean all data input into or made available by Customer for processing within the Services or generated from the Services.

"Customer Personal Data" means any personal data contained in Customer Data or provided by (or on behalf of) Customer to Apollo in connection with the Services. Unless expressly set forth otherwise in the Agreement or an applicable Order, Customer Personal Data does not include Barred Data (as defined in the Agreement).

"EEA" means the European Economic Area.

"EU Data Protection Laws" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (the **"EU GDPR"**); (ii) in respect of the United Kingdom, the EU GDPR 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) (the **"UK GDPR"**); and (iii) the Swiss Federal Data Protection Act (**"Swiss DPA"**).

"Information Security Incident" means a confirmed breach of Apollo's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of (or access to), Customer Personal Data in Provider's possession, custody, or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

"Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"Standard Contractual Clauses" means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 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 ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and

(iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs").

"Services" means the provision of the Apollo Platform (and/or other Apollo hosted solutions or cloud products, if applicable) by Apollo to Customer pursuant to the Agreement.

"Subprocessor" means any processor engaged by Apollo to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data. Subprocessors may include Apollo's affiliates or other third parties.

"U.S. Data Protection Law" means all data protection or privacy laws and regulations applicable to the Customer Personal Data in question in force within the United States, including the California Consumer Privacy Act (as may be amended from time to time) (the **"CCPA"**), and any rules or regulations implementing the foregoing.

2. Scope and relationship of the parties. As applicable, this DPA applies when Customer Personal Data is processed by Apollo as a processor or subprocessor in its provision of the Services to Customer, who will act as either a controller or processor of the Customer Personal Data.

3. Details of Processing. The details of the processing of Customer Personal Data by Apollo is described in Annex A to this DPA. Customer agrees that this Annex A can be updated by Apollo from time to time as necessary for Apollo to reflect new products, features, or functionality of the Services.

4. Customer Instructions and Apollo Processing. Apollo shall process Customer Personal Data as a processor, only in accordance with Customer's documented lawful instructions and as necessary to perform its obligations under the Agreement. Customer instructs Apollo to process Customer Personal Data for the following purposes: (a) processing in accordance with the Agreement and any applicable Order(s); (b) processing initiated by Customer and/or Customer's end-users of the Services ("Users") in their use or configuration of the Services; and (c) processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement (subsections (a)-(c), the "Permitted Purpose"). Apollo shall not "sell" the Customer Personal Data within the meaning of the CCPA or otherwise. For clarity, Apollo is not responsible for determining if Customer's instructions are compliant with applicable laws. However, Apollo shall notify Customer in writing if, in its reasonable opinion, the Customer's processing instructions violate Applicable Data Protection Laws.

5. Customer Obligations. Customer agrees that it shall have sole responsibility for the accuracy and quality of Customer Personal Data, and for providing any notices and obtaining any consents, permissions and rights required to enable Apollo to process Customer Personal Data. Customer shall ensure that its instructions and processing of Customer Personal Data comply with Applicable Data Protection Laws.

6. Data Transfers.

a) Hosting and Processing Locations. Apollo will only host Customer Personal Data in the United States or such other region(s) that are offered by Apollo and agreed with Customer on an Order (the "Hosting Region"). Customer is solely responsible for the regions from which its Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its Users and for any subsequent designation of other Hosting Regions. Once the Hosting Region is agreed upon, Apollo will not process Customer Personal Data from outside the Hosting Region except as necessary to comply with the law or binding order of a governmental body.

b) Transfer Mechanisms. The parties agree that when the transfer of Customer Personal Data by Customer (as "data exporter") to Apollo (as "data importer") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, it shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA, as follows:

i) In relation to transfers of Customer Personal Data protected by the EU GDPR and processed in accordance with this DPA, the EU SCCs shall apply, completed as follows:

1) Module Two or Module Three will apply (as applicable);
2) in Clause 7, the optional docking clause will not apply;
3) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 7 of this DPA;
4) in Clause 11, the optional language will not apply;
5) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

6) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
7) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA, as applicable; and
8) Subject to Section 8 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA.

ii) In relation to transfers of Customer Personal Data protected by the UK GDPR, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

1) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;
2) references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;
3) Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts," unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the UK GDPR in which case the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in Annex A and Annex B of this DPA (as applicable).

iii) In relation to transfers of Customer Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

1) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;
2) references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and
3) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland, unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss DPA in which case the Swiss SCCS shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Annex A and Annex B to this DPA (as applicable).

iv) It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

7. Subprocessing.

a) Subprocessors. Customer provides a general authorization for Apollo to engage Subprocessors to process Customer Personal Data in accordance with this DPA, including the Subprocessors currently engaged by Apollo and listed at the following URL: https://www.apollographql.com/docs/studio/sub-processors/ ("Subprocessor Site"). Apollo will: (i) enter into written agreements with its Subprocessor imposing data protection and security measures no less protective of Customer Personal Data than the Agreement and this DPA; and (ii) remain responsible to Customer for any breach of the Agreement and this DPA that is caused by an act, error, or omission of its Subprocessors, to the extent Apollo would have been liable for such act, error, or omission had it been caused by Apollo.

b) Changes to Subprocessors. Apollo shall (i) update the Subprocessor Site when it has appointed any new Subprocessors; and (ii) notify Customer if it adds any new and relevant Subprocessors at least fourteen (14) days' prior to allowing such Subprocessor to process Customer Personal Data. When available, Customer must subscribe to receive notice of updates to the Subprocessor Site, using a mechanism available on the Subprocessor Site. Customer may object (in writing at legal@apollographql.com) to Apollo's appointment of a new Subprocessor within five (5) calendar days after receiving notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss

such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the Agreement (including this DPA) for convenience.

8. Security.

a) Security Measures. Apollo shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Information Security Incidents and to preserve the security and confidentiality of the Customer Personal Data in accordance with Apollo's Security Policy, as defined in the Agreement. Apollo may review and update its Security Policy from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data or otherwise amend this DPA or Apollo's obligations pertaining to the Processing of Customer Personal Data.

b) Confidentiality. Apollo shall ensure that any person who is authorised by Apollo to process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

c) No Assessment of Customer Personal Data by Apollo. Apollo shall have no obligation to assess the contents of Customer Personal Data to identify information subject to any specific legal requirements. Customer is responsible for reviewing the information made available by Apollo relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Applicable Data Protection Laws

9. Assistance and Cooperation:

a) Data Subject Requests. To the extent legally permitted, Apollo shall promptly notify Customer if Apollo receives a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Customer Personal Data, or to restrict the Processing of Customer Personal Data ("Data Subject Request"). The Services provide or may provide Customer with applicable controls that Customer may use to assist it in responding to a Data Subject Request and Customer will be responsible for responding to any such Data Subject Request. To the extent Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, taking into account the nature of the Processing, Apollo shall (upon Customer's written request) provide commercially reasonable cooperation to assist Customer in responding to any Data Subject Requests.

b) Data Protection Impact Assessments. Apollo will provide commercially reasonable assistance to Customer (at Customer's expense) with respect to any legally required data protection impact assessment relating to the processing or proposed processing of Customer Personal Data in connection with the Services and any related required consultation with supervisory authorities.

c) Law Enforcement or Third-Party Demands. If Apollo receives a demand to retain, disclose, or otherwise process Customer Personal Data for any third party, including, but not limited to law enforcement or a government authority ("**Third-Party Demand**"), then Apollo shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Apollo can provide information to such third party as reasonably necessary to redirect the Third-Party Demand. If Apollo cannot redirect the Third-Party Demand to Customer, then Apollo shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy.

10. Information Security incidents. Upon becoming aware of an Information Security Incident, Apollo shall inform Customer without undue delay and shall provide timely information relating to the Information Security Incident as it becomes known or as is reasonably requested by Customer to allow Customer to fulfil its data breach reporting obligations under Applicable Data Protection Law. Customer shall further take reasonable steps to contain, investigate, and mitigate the effects of the Information Security Incident. Apollo's notification of or response to an Information Security Incident in accordance with this Section 10 will not be construed as an acknowledgment by Apollo of any fault or liability with respect to the Information Security Incident.

11. **Return or Deletion of Customer Personal Data.** Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the Agreement as set forth in the Agreement. Subject to Section 9(c), any Customer Personal Data not deleted by Customer shall be deleted by Apollo promptly upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "Retrieval Right" set forth in the Agreement.

12. **Audit.** Customer may audit Apollo's compliance with its obligations under this DPA up to once per calendar year and on such other occasions as may be required by EU Data Protection Laws, including where 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 in the circumstances 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 objection by Apollo will require Customer to appoint another auditor or conduct the audit itself. In the event that Customer (acting reasonably) is able to provide documentary evidence that the information made available by Apollo is not sufficient in the circumstances 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 in relation to the processing of the 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 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. Apollo will review the proposed audit plan and provide Customer with any concerns or questions (for example, 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 12 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 twelve (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, and hereby indemnifies Apollo in respect of, any damage, injury or disruption to Provider'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 services to such other customers). Customer will promptly notify Provider of any non-compliance discovered during the course of an audit and provide Provider any audit reports generated in connection with any audit under this Section 12, unless prohibited by EU 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. Any audits are at Customer's sole expense.

13. **Relationship with the Agreement:**

a) The parties agree that this DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.
b) Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data. If there is any conflict between the Standard Contractual Clauses and the Agreement (including this DPA), the Standard Contractual Clauses shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data.
c) Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.
d) Any claims against Apollo under this DPA shall only be brought by the Customer entity that is a party to the Agreement against Apollo. In no event shall this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.
e) This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.
f) This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically upon deletion by Apollo of the personal data covered by this DPA, in accordance with Section 13 of this DPA.

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

Customer:_____	**Apollo Graph, Inc.**
Signature:_____	Signature:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date Signed:_____	Date Signed:_____
Contact Email:_____	Contact Email: legal@apollographql.com

ANNEX A

List of Parties / Description of Processing / Transfer

Annex 1(A): List of Parties	
Data Exporter	**Name of the data exporter:** the entity identified as "Customer" on the Agreement **Contact details:** the address and contact details associated with Customer's Apollo account, or as otherwise specified in the Agreement or this DPA. **Activities relevant to the data transferred:** See Annex 1(B) below. User access to Apollo's cloud-based, subscription access to Apollo's graphQL hosted analytical tools and related services, as further described in the Agreement. **Signature and date:** See DPA signature page **Role (Controller/Processor):** Controller for Module 2; Processor for Module 3
Data Importer	**Name of the data exporter:** Apollo Graph, Inc. **Contact details:** Legal Department; legal@apollographql.com **Activities relevant to the data transferred:** See Annex 1(B) below. Apollo provides a cloud-based, subscription access to Apollo's graphQL hosted analytical tools and related services, as further described in the Agreement. **Signature and date:** See DPA signature page **Role (Controller/Processor):** Processor
Annex 1(B): Description of the Processing / Transfer	
Categories of data subjects whose personal data is transferred:	Users of the Services
Categories of personal data transferred:	Business Contact Information as defined in the Agreement
Sensitive data transferred (if appropriate):	Not Applicable
Frequency of the transfer:	Continuous
Nature of the processing:	Providing the Services (including support and technical services) as permitted in the Agreement, including User login and authentication, to maintain and display User profiles, and manage access controls and User permissions. Providing routine business communications in accordance with Apollo's privacy policy located at the URL https://www.apollographql.com/Apollo-Privacy-Policy.pdf
Purpose(s) of the data transfer:	Permitted Purposes as set forth in Section 4 of the DPA
Duration of the processing:	Apollo will retain Customer Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Apollo is obligated to process Customer Personal Data in accordance with the Agreement.
Transfers to Subprocessors:	A list of Subprocessor providing services related to infrastructure and provision of the Services as described in Annex B
Annex 1(C): Competent Supervisory Authority	
Competent supervisory authority:	Irish DPC

ANNEX B

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Apollo maintains the technical and organizational security measures described in Section 8 in the DPA

***For transfers to Subprocessors**, also describe the specific technical and organisational measures to be taken by the Subprocessor to be able to provide assistance to the controller and, for transfers from a processor to a Subprocessor, to the data exporter:*

Subprocessor	Location	Role	Security Measures
Google Cloud	*United States*	*Hosting Provider and Analytics Tool*	*https://cloud.google.com/security/gdpr* *https://cloud.google.com/security/infrastructure/design*
PingOne	*United States*	*User Management*	*https://www.pingidentity.com/en/company/security-at-ping-identity.html*
GitHub	*United States*	*User Management*	*https://github.com/security*