PALANTIR DATA PROTECTION ADDENDUM ("DPA")

The customer agreeing to the terms of this DPA ("**Customer**") and the Palantir Technologies entity that is the signatory to the Agreement ("**Palantir**"; each of Customer and Palantir a "**Party**" and collectively the "**Parties**"), have entered into an agreement (such as the Palantir Terms of Service and Order Form) governing Customer's use of Palantir Technology, including the Service, and the provision of related Professional Services to Customer by Palantir, including any attachments, order forms, exhibits, and appendices thereto (collectively, the "**Agreement**"). This DPA supplements, is incorporated into, and forms part of the Agreement and establishes the rights and obligations of Palantir and Customer with respect to any Customer Personal Data Processed by Palantir on behalf of Customer under the Agreement. Any capitalized terms used but not defined in this DPA shall have the meaning provided in the Agreement. To the extent there is any conflict in meaning between any provisions of the Agreement and this DPA, the terms and conditions in this DPA shall prevail and control.

1. DEFINITIONS

1.1 The following capitalized terms will have the meanings indicated below:

- **"Adequate Country"** means a country that may import Personal Data and is deemed by the governing authority of the exporting country to provide an adequate level of data protection under the applicable Data Protection Laws;

- "**Affiliate**" means an entity that, directly or indirectly, owns or controls or is owned or controlled by, or is under common ownership or control with, a Party. As used herein, "control" means the power to direct, directly or indirectly, the management or affairs of an entity and "ownership" means the beneficial ownership of more than fifty percent of the voting equity securities or other equivalent voting interests of an entity. In respect of Palantir, Affiliate shall include, without being limited to, all entities listed in Exhibit A, Part II and any other Palantir affiliates from time to time;

- "**Completions**" has the meaning given to it in Exhibit D of this DPA;

- "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data and includes, as applicable, the term "controller" "business" and any other similar or equivalent terms under applicable Data Protection Laws;

- "**Customer Personal Data**" means any Personal Data contained within Customer Data subject to Data Protection Laws that Customer, including Users, provides or makes available to Palantir in connection with the Agreement;

- "**Data Incident**" means any breach, as defined by applicable Data Protection Laws, of Palantir's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data on systems managed or otherwise controlled by Palantir;

- "**Data Protection Authority**" means a competent authority responsible for enforcing the application of the relevant Data Protection Laws, and includes, as applicable, any data protection authority, privacy regulator, supervisory authority, Attorney General, state privacy agency or any governmental body or agency enforcing Data Protection Laws;

- "**Data Protection Laws**" means all laws and regulations as amended from time to time regarding data protection, consumer privacy, electronic communications and marketing laws to the extent applicable to the Processing of Customer Personal Data by Palantir under the Agreement, such as:

  - Federal and state privacy laws, and their implementing regulations, as amended or superseded from time to time, to the extent they apply to the processing of Personal Data in the US ("**US Privacy Laws**"). State comprehensive consumer privacy laws include, but are not limited to, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**");

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**EU GDPR**"); and

- The EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 ("**UK GDPR**");

- "**Data Protection Officer**" means the natural person or company appointed where necessary under applicable Data Protection Laws to ensure an organization's compliance with Data Protection Laws and cooperate with the Data Protection Authorities;

- "**Data Subject**" means the identified or identifiable person to whom Personal Data relates, and includes, as applicable, the term "consumer" and any other similar or equivalent terms under Applicable Data Protection Laws;

- "**DPA Effective Date"** means the Effective Date of the Agreement;

- "**EEA**" means the European Economic Area;

- "**EU SCCs**" means the standard contractual clauses for use in relation to exports of Personal Data from the EEA approved by the European Commission under Commission Implementing Decision 2021/914, or such other clauses as replace them from time to time;

- "**Personal Data**" means: (a) any information relating to (i) an identified or identifiable natural person and/or (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws), and (b) any information treated or receiving similar treatment as "personal data", "personal information", "personally identifiable information or any similar, or equivalent terms under applicable Data Protection Laws;

- "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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. The terms "process", "processes" and "processed" will be interpreted accordingly;

- "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable the terms "processor", "service provider" and any equivalent or similar terms that address the same, or similar, responsibilities under applicable Data Protection Laws;

- "**Request**" means a request from a Data Subject or anyone acting on their behalf to exercise their rights under Data Protection Laws;

- "**Restricted Transfer**" means a transfer, or onward transfer, of Personal Data from a country where such transfer would be restricted or prohibited by applicable Data Protection Laws (or by the terms of a data transfer agreement put in place to address the data transfer restrictions of Data Protection Laws) without implementing safeguards such as the Standard Contractual Clauses to be established under clause 14 below;

- "**Security Documentation**" means the Documentation describing the security standards that apply to the Service as provided by or on behalf of Palantir from time to time;

- "**Sell**" or "**Sale**" shall have the meaning prescribed by applicable US Privacy Laws;

- "**Service**" shall have the meaning as set out in the Agreement and this DPA;

- **"Share"** shall have the meaning as prescribed by the CCPA;

- "**Subprocessor**" means any processor or service provider who processes personal data on behalf of Palantir for the purpose of providing the Service as set out in the Agreement, Exhibit A and any other relevant applicable exhibits of this DPA;

- "**Standard Contractual Clauses**" or "**SCCs**" means either (a) the standard data protection clauses approved pursuant to the Data Protection Laws of the applicable exporting country from time to time to legitimise exports of Personal Data from that country, or (b) where the applicable exporting country has Data Protection Laws that regulate the export of personal data but no approved standard data protection clauses, the EU SCCs shall apply- in each case incorporating the appropriate Completions, and where more than one form of such approved clauses exists in respect of a particular country, the clauses that shall apply shall be: (i) in respect of any situation where Customer acts as a Controller of Customer Personal Data, that form of clauses applying to Controller to Processor transfers; and (ii) in respect of any situation where Customer acts as a Processor of Customer Personal Data, that form of clauses applying to Processor to Processor transfers; and

- "**Technical and Organisational Measures**" means the technical and organisational measures agreed by the Parties in the Agreement and any additional technical and organisational measures implemented by Palantir pursuant to its obligations under applicable Data Protection Laws.

2. TERM

2.1 This DPA will take effect from the DPA Effective Date and remain in effect until the destruction or return of all Customer Personal Data by Palantir in accordance with the Agreement, at which point it will automatically terminate.

3. SCOPE AND APPLICATION

3.1 This DPA is incorporated into, and forms part of, the Agreement and establishes the rights and obligations of Palantir and Customer with respect to any Customer Personal Data Processed by Palantir on behalf of Customer when in the course of the provision of the Service. To the extent there is any conflict in meaning between any provisions of the Agreement and this DPA, the provisions in this DPA shall prevail and control.

4. ROLE OF THE PARTIES

4.1 Customer and any relevant Customer Affiliate, hereby appoints and instructs Palantir as a Processor, or Subprocessor as applicable, of the Customer Personal Data. Accordingly, the Parties shall comply with applicable Data Protection Laws as relevant to their respective Processing of Customer Personal Data under the Agreement.

4.2 As between the Parties, Customer shall be liable and responsible as the Controller (or Processor, if Customer is Processing Personal Data with the Service for a third-party Controller) and Palantir shall be liable and responsible as the Processor (or Subprocessor), in respect of Customer Personal Data. In the event that Customer acts as a Processor (or Subprocessor) in respect of Customer Personal Data, Customer represents and warrants to Palantir that it is validly authorized by the relevant Controller to enter into the Agreement and this DPA and to provide Customer Instructions (as defined below) on behalf of the Controller in relation to Customer Personal Data.

4.3 The subject matter and details of Processing are described in the Agreement and this DPA, including Exhibit B (subject matter and details of Customer Personal Data processing) and any other relevant exhibits for applicable additional Services.

5. CUSTOMER PROCESSING OF PERSONAL DATA

5.1 Customer shall ensure that any Processing of Customer Personal Data via Customer's use of the Service, including any instructions provided to Palantir in relation to such Processing, shall comply with all applicable Data Protection Laws.

5.2 Customer instructs Palantir to Process Customer Personal Data: (a) to provide the Service specified in the Agreement and Documentation or otherwise perform its obligations thereunder; (b) as further initiated by Customer via Customer's or Users use of the Service in accordance with the Agreement and Documentation; and/or (c) in accordance with any additional instruction outside the scope of the Agreement or this DPA, as further documented in any other written instructions given by Customer and acknowledged by Palantir in writing as constituting instructions for purposes of this DPA (collectively, "Customer Instructions"). Customer acknowledges that any additional Customer Instructions issued under (c) above may result in additional charges or fees to the Customer by Palantir, which shall be payable in accordance with the terms of the Agreement.

5.3 Customer shall have sole responsibility for the lawful Processing of Customer Personal Data in connection with its use of the Palantir Technology and/or its receipt of any related Professional Services in accordance with applicable Data Protection Laws, including without limitation, the accuracy, quality, and legality of the Customer Personal Data, the means by which it acquires and uses Customer Personal Data, and the Customer Instructions regarding the Processing of Customer Personal Data. Customer represents and warrants that it has (or its Controller has) a valid legal basis for the Processing of Customer Personal Data and has (or its Controller has) provided (or procured the provision of) all notifications and obtained (or procured the provision of) all consents (including Consents), authorizations, approvals, and/or agreements (including, where Customer is a Processor or Subprocessor, with and from the applicable Controller(s)) required under applicable laws or policies in order to enable Palantir to receive and Process Customer Personal Data in accordance with this DPA, the Agreement and Customer Instructions.

6. PALANTIR PROCESSING OF CUSTOMER PERSONAL DATA

6.1 Palantir will Process Customer Personal Data for the business purposes of providing to Customer the services, namely the Palantir Technology and Professional Services pursuant to the Customer Instructions ("Business Purposes"), in accordance with the terms of the Agreement and this DPA as well as any requirements set out by applicable Data Protection Laws. For the avoidance of doubt, Customer is disclosing Customer Personal Data to Palantir only for the limited and specified Business Purposes set forth within the Agreement and the Customer Instructions. Palantir shall process Customer personal Data pursuant to Customer's instructions and shall:

> (a) designate and maintain a Data Protection Officer as required by Data Protection Laws as they pertain to Processors, which can be contacted at privacy@palantir.com;

> (b) not Sell or Share Customer Personal Data or otherwise retain, use, disclose, or Process Customer Personal Data outside of the direct business relationship between the Parties or for any purpose other than for the fulfilment of the Business Purposes pursuant to Customer Instructions, unless obligated to do otherwise by applicable law or regulation or requests or orders of judicial, governmental or regulatory entities (including without limitation subpoenas), in which case Palantir will inform Customer of that legal requirement before such Processing occurs unless legally prohibited from doing so;

> (c) to the extent required by the CCPA, not combine Customer Personal Data with Personal Data that it receives from other sources or collects from its own interactions with a Data Subject, provided, however, that Palantir may combine Customer Personal Data as necessary to perform its internal business purposes in connection only with the provision of the Service;

> (d) implement appropriate Technical and Organisational Measures as described in the Security Documentation to ensure a level of security appropriate to the risk against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. To the extent such assistance requires Palantir to take additional steps beyond those imposed on Palantir by Data Protection Laws or specifically required pursuant to the Agreement; or to the extent the relevant technical and organizational measures are required as a result of an act or omission by Customer or a Party acting on behalf of Customer in breach of this Agreement or Data Protection Laws, then Palantir's obligation to provide such assistance shall be subject to Customer's payment of Palantir's reasonable fees in respect of such additional assistance;

> (e) ensure that all persons authorized by Palantir to Process Customer Personal Data, including any Subprocessors (as defined below), are bound by confidentiality obligations consistent with those set out in this DPA, the Agreement or otherwise sufficient to meet the requirements of Data Protection Laws;

> (f) where applicable, notify the Customer if it can no longer meet its obligations under CCPA and is unable to cure within a reasonable period of time;

> (g) take reasonable steps to return or destroy Customer Personal Data at the choice of the Customer, when it is no longer necessary for the purposes of performing the relevant Services upon termination of the Agreement, unless storage is otherwise required under applicable Data Protection Laws; and

> (h) process Customer Personal Data in a manner that is consistent with the same level of privacy protection that is required of Customer under applicable Data Protection Laws.

6.2. Customer shall instruct Palantir as to the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects taking into account the specific tasks and responsibilities of the

Processor in the context of the Processing to be carried out and the risk to the rights and freedoms of the Data Subject as part of Customer Instructions. Notwithstanding anything to the contrary herein, Customer shall ensure that its acts or omissions, including in relation to any Customer Instructions to Palantir, do not put Palantir in breach of the Data Protection Laws.

6.3 Customer has assessed the level of security appropriate to the Processing in the context of its obligations under Data Protection Laws and agrees that the Technical and Organisational Measures are consistent with such assessment. Customer further acknowledges that Palantir is not able to assess, and does not have knowledge of, the specific Personal Data provided by Customer to Palantir or made available by Customer to Palantir in relation to the Services and that as a result the technical and organisational Measures proposed by Palantir are generic in nature and Palantir is unable to assess whether or not they reflect any particular risks posed by the Personal Data.

7. SUBPROCESSORS

7.1 Customer provides a general authorization to Palantir, where applicable, to engage Subprocessors listed in Exhibit A, provided that, prior to permitting such Subprocessors to Process any Customer Personal Data, Palantir shall enter into a written agreement with the Subprocessor including terms that are consistent with those set out in this DPA, or otherwise sufficient to meet the requirements of Data Protection Laws.

7.2 Subject to Section 7.1, Palantir shall, prior to the appointment of any Subprocessor to Process Personal Data, provide Customer with advance written notice within a reasonable period prior to the proposed engagement, specifying the identity, location, and nature of processing to be undertaken. Notification may be provided through the Service, via email, or any other reasonable means. Where, and to the extent that, Customer has a right to object to the engagement of a Subprocessor under applicable Data Protection Laws, Customer may object on reasonable grounds relating to data protection by providing written notice detailing the grounds for objection within the notice period. Where Customer objects by providing written notice detailing the grounds of such objection, the Parties agree to cooperate in good faith to address Customer's objection. If the Parties cannot resolve Customer's objections, Customer may exercise its right to terminate under the Agreement.

7.3 To the extent required by applicable Data Protection Laws, Palantir shall remain liable to Customer for the performance of the Subprocessor's obligations in relation to this Section 7 ("**Subprocessor Data Protection Liability**"), and Palantir shall be permitted to re-perform or to procure the re-performance of any such obligations and Customer acknowledges that such re-performance shall diminish any claim that Customer has against Palantir in respect of any Subprocessor Data Protection Liability.

8. AUDIT

8.1 Palantir uses third party auditors to verify the adequacy of its security measures. This audit is performed at least annually, by independent and reputable third-party auditors at Palantir's selection and expense, and in accordance with Service Organization Controls 2 (SOC2) or substantially equivalent industry standards, and results in the generation of an audit report ("Report") which will be the Confidential Information of Palantir. The Service and operations are also certified compliant with the standards and accreditations set out on the "compliance and accreditation" tab at: https://www.palantir.com/information-security/ ("**Accreditations**").

8.2 Palantir will provide information reasonably necessary to demonstrate compliance with this DPA and applicable Data Protection Laws upon Customer's reasonable request. At Customer's written request, Palantir will provide Customer with a confidential summary of the Report, documentation evidencing compliance with the Accreditations, and the Accountability Information outlined in Section 10 of this DPA so that Customer can reasonably verify Palantir's compliance with the data security and data protection obligations under this DPA. Subject to Section 8.3, if Data Protection Laws, Standard Contractual Clauses, or the Agreement provide the right for Customer to obtain an audit of Palantir facilities or information in addition to the Report and the Accountability Information, then Customer has the right to request or mandate on its own behalf Palantir to carry out such audit. Palantir will then follow the instructions provided by Customer with respect to such audit, whose scope should be limited to Palantir's compliance with the terms and conditions of this DPA as it applies to Customer Personal Data to the extent expressly required by the Agreement, the Standard Contractual Clauses, or Data Protection Laws.

8.3 In order to request an audit of Palantir's facilities under this Section 8 (and where such an audit is authorized), Customer shall notify Palantir in writing and the Parties shall agree in writing, as soon as reasonably possible but always in advance, on the conditions of the audit, including but not limited to the dates and scope of the audit. Customer may conduct one (1) audit per calendar year, unless otherwise required by applicable law or a Data Protection Authority. Palantir may decline the request or decline to follow any instruction requested by Customer regarding audits. To the extent Palantir declines to follow any instruction requested by Customer regarding audits and an audit right is unambiguously granted to Customer under applicable Data Protection Laws, Customer is entitled to

terminate the Agreement in accordance with the Agreement. The Customer shall bear the reasonable costs of Palantir in fulfilling any requirements under this Section. The scope of any audit under this Section 8 shall be limited to Palantir systems and facilities used to Process Customer Personal Data and Documentation directly related to such Processing.

8.4 All information provided or made available to Customer, its auditor or any other third-party authorized under the present DPA to have access to the above information pursuant to this Section 8 shall be Confidential Information of Palantir.

8.5 In the event of any confirmed material non-compliance by Palantir with the terms of this DPA, Customer may take reasonable steps to remediate the same, including, without limitation, by requiring the suspension of all Processing of Customer Personal Data until such time as Customer determines that the non-compliance has been remediated. In the event that Palantir determines that it can no longer meet its obligations pursuant to this DPA, Palantir shall promptly notify Customer of such determination.

9. DEALINGS WITH DATA PROTECTION AUTHORITIES AND DATA PROTECTION IMPACT ASSESSMENTS

9.1 Palantir shall reasonably cooperate, on reasonable request and at Customer's cost, with any Data Protection Authority in the performance of its tasks, taking into account the nature of the Processing by, and information available to, Palantir.

9.2 Taking into account the nature of the Service and the information available to Palantir, Palantir will assist Customer in complying with Customer's obligations in respect of data protection impact assessments (including a 'risk assessment', 'privacy impact assessment', 'data protection assessment' or any equivalent documentation) and prior consultation or mandatory submission to a Data Protection Authority where applicable under Data Protection Laws, by providing the Report, Accountability Information and Documentation.

10. ACCOUNTABILITY

10.1 To the extent required by Data Protection Laws, Palantir shall maintain electronic records of all categories of Processing activities carried out on behalf of Customer, containing:

> (a) the name and contact details of the Processors and Subprocessors;
>
> (b) details of the types of Processing being carried out;
>
> (c) details of any transfers of Customer Personal Data to a territory or international organisation outside of the EEA or UK, and documentation of suitable safeguards (if applicable); and
>
> (d) a general description of the technical and organisational security measures used in relation to the Processing,

together, the "**Accountability Information**".

11. DATA SUBJECT RIGHTS

11.1 With regard to Customer Personal Data, where Palantir directly receives a Request from a Data Subject, or anyone authorized to act on their behalf, any claim or complaint in relation to their rights under the Data Protection Laws, and provided Palantir can reasonably identify from the information provided that the request, claim or complaint relates to Customer and Customer Personal Data, then unless prohibited by applicable law, Palantir shall forward the request, claim or complaint to Customer.

11.2 On reasonable written request from Customer, and taking into account the nature of the Processing, Palantir shall use commercially reasonable efforts to offers Customer certain controls as described in the Documentation that Customer may elect to use to comply with its obligations towards Data Subjects.

12. DATA INCIDENT

12.1 Palantir shall notify Customer without undue delay after becoming aware of (or where required by applicable Data Protection Laws) having reasonable grounds to believe that there has been a Data Incident and provide Customer with any information required to be included under applicable Data Protection Laws. For avoidance of doubt, a Data Incident shall not include acts or omissions which do not breach Palantir's security or the security of any Subprocessor; port scans, authorized penetration tests, and denial of service attacks; or any access to or Processing of Customer Personal Data that is consistent with Customer Instructions.

12.2 Palantir shall provide Customer with reasonable cooperation and assistance in dealing with a Data Incident, in particular in relation to (a) taking commercially reasonable steps to resolve any data privacy or security issues involving any Customer Personal Data; and (b) making any appropriate notifications to individuals affected by the Data Incident or to a Supervisory Authority to the extent

reasonably possible; provided that, Customer shall maintain and follow an effective cyber incident response policy, which shall include the use of legal professional, litigation, or client attorney privilege, work in good faith with Palantir in relation to the Data Incident, and agree with Palantir the form and method of any public announcement in relation to the Data Incident.

12.3 Any information provided by Palantir pursuant to this Section 12 shall be the Confidential Information of Palantir and Palantir's notification of or response to a Data Incident under this Section 12 will not be construed as an acknowledgement by Palantir or, if relevant, its Subprocessors of any fault or liability with respect to the performance of any Service or Professional Services (as applicable).

13. DATA TRANSFERS

13.1 Palantir may Process Personal Data in countries outside of the country in which Customer is established in which Palantir or its Subprocessors maintains facilities, employees or infrastructure.

13.2 Where the Processing of Customer Personal Data in the course of the provision of the Service involves a Restricted Transfer of Customer Personal Data by or on behalf of Customer, from a country which places restrictions on the transfer of Personal Data to countries not deemed to be an Adequate Country then:

(a) Palantir shall provide appropriate safeguards, meeting the requirements of the applicable SCCs in respect of onward transfers, in relation to transfers of the Personal Data between Palantir Affiliates for the purpose of performing Services; and

(b) Palantir shall ensure that any transfers of Customer Personal Data between Palantir and any Palantir third party Subprocessors, are subject to contractual terms between Palantir and the relevant third party Subprocessor providing appropriate safeguards and containing clauses equivalent to the SCCs; or

(c) Where the Parties choose to enter into SCCs, the applicable SCCs and any required Completions as applicable and set out in Exhibit D, shall hereby be deemed incorporated into this DPA, and apply between Customer (as Exporter) and Palantir (as importer),

13.3 Nothing in this DPA or the Agreement modifies any rights or obligations of Palantir or customer under the Standard Contractual Clauses.

14. LIABILITY

14.1 Subject to 14.2, the total combined liability of either Party and its Affiliates towards the other Party and its Affiliates under or in connection with the Agreement and the Standard Contractual Clauses combined will be the liability cap, and subject to the liability limitations, set forth in the Agreement for the relevant Party.

14.2 Nothing in this DPA serves to modify, disapply or amend the terms of the Agreement relating to liability, including but not limited to any exclusions and/or limitations of liability.

14.3 Customer shall ensure that all Customer Data it uploads in the course of the provision of the Service is accurate and complies with all applicable laws. Palantir does not monitor or control any Customer Data on Palantir Services. Customer shall defend and indemnify Palantir for any and all damages, liabilities, penalties, fines and expenses (including from third parties) arising out of the Customer's failure to comply with the present provision or any applicable laws in connection with Customer Data.

15. GOVERNING LAW AND JURISDICTION

15.1 The Parties shall modify the terms of this DPA as soon as possible if such modification is required for the parties to comply with any Data Protection Laws, or in order to implement or adhere to the Standard Contractual Clauses or such other permitted compliance mechanism under Data Protection Laws.

15.2 This DPA, and any dispute or claim (including any non-contractual disputes or claims) arising out of or in connection with it, or its subject matter or formation, shall be governed by and construed in accordance with the laws that govern the Agreement. If it is or becomes a requirement that, under the Data Protection Laws or other applicable laws, this DPA must be governed by (a) the laws of a member state of the European Union (and it is not already so governed), this DPA shall be governed by and construed in accordance with the laws of Ireland; (b) the laws of the United Kingdom, this DPA shall be governed by and construed in accordance with the laws of England and Wales, and/or (c) the laws of any other jurisdiction, then this DPA shall be governed by and construed in accordance with the laws of that jurisdiction, but only to the extent required to satisfy such laws.

15.3 The Parties irrevocably agree that the forum set out in the Agreement shall have exclusive jurisdiction to settle any dispute which may arise out of or in connection with this DPA and the documents to be entered into pursuant to it and that, accordingly, any proceedings arising out of or in connection with this DPA shall be brought in such forum save that where a mandatory requirement of Data Protection Law or other applicable laws requires that disputes arising out of or in connection with this DPA and any documents to be entered into pursuant to it are heard in (a) a member state of the European Union, then such disputes shall be heard in Ireland; (b) the United Kingdom, then such disputes shall be heard in England and Wales; and/or (c) any alternative forum, then such disputes shall be heard in that alternative forum, to the extent legally permitted. Each of the Parties irrevocably submits to the jurisdiction of such forum and waives any objection to proceedings in any such forum on the ground of venue or on the ground that proceedings have been brought in an inconvenient forum.

16. GENERAL TERMS

16.1 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, whilst preserving the Parties' intension as closely as possible, or, where not possible, (ii) construed in a manner as if the invalid off unenforceable part had never been contained therein.

16.2 Palantir may notify Customer in writing from time to time of any variations to this DPA, including relating to cross border transfers, which are required as a result of change in Data Protection Laws.

EXHIBIT A

List of approved Subprocessors

PART I - Subprocessors

To perform its obligations under the Palantir Terms of Service and Palantir Data Protection Agreement (or the alternative written agreement between Customer and Palantir, if applicable), Palantir Technologies Inc. and its Affiliates may use third-party data processors ("**Third-Party Subprocessors**") and Palantir Affiliates to process Customer Personal Data. Capitalized terms used but not defined here shall have the meanings provided in the Agreement.

The following third parties are hereby specifically authorized by Customer to carry out work as Third-Party Subprocessors for purposes of the Agreement.

Authorized Third-Party Subprocessors				
Subprocessor	**Purpose**	**Registered Address**	**Location**	**Transfer Mechanism**
Amazon Web Services, Inc.	Cloud hosting and infrastructure, alerting and encrypted notification services and AI services.	410 Terry Avenue North, Seattle, WA 98109, USA	As selected by Customer in the Order Form or, as applicable, other parts of the Agreement	Standard Contractual Clauses
Microsoft Corporation	Cloud hosting and infrastructure and AI services (Microsoft Azure).	One Microsoft Way, Redmond, WA 98052, USA	The location for the purpose of providing the cloud hosting service is as selected by Customer in the Order Form or, as applicable, other parts of the Agreement. The location for the purpose	Standard Contractual Clauses

			of providing the AI service is East US, South Central US, West Europe and other Azure regions as they become available.	
Google LLC	Cloud hosting and infrastructure (Google Cloud Platform) and AI services.	1600 Amphitheatre Parkway, Mountain View, 94043 CA, USA	The location for the purpose of providing the cloud hosting service is as selected by Customer in the Order Form or, as applicable, other parts of the Agreement. The location for the purpose of providing the AI services are all regions available for features of Generative AI on Google Vertex AI and other regions as they become available.	Standard Contractual Clauses
Microsoft Corporation	User authentication as an identity provider (where selected as chosen identity provider by Customer).	One Microsoft Way, Redmond, WA 98052, USA	United States	Standard Contractual Clauses
OpenAI LLC	AI services.	3180 18th Street, San Francisco, CA 94110, USA	The location for the purpose of providing the AI service can be the United States and other regions as they become available.	Standard Contractual Clauses
X.AI LLC	AI services.	1450 Page Mill Rd, Palo Alto, CA 94034, USA	The location for the purpose of providing the AI service can be the United States and other regions as they become available.	Standard Contractual Clauses
Oracle America, Inc.	Cloud hosting and infrastructure.	500 Oracle Parkway, Redwood Shores, CA 94065, USA	As selected by Customer in the Order Form or, as applicable, other parts of the Agreement	Standard Contractual Clauses

Anthropic, PBC	AI services.	548 Market Street, PMB 90375, San Francisco, CA 94104-5401, USA	The location for the purpose of providing the AI service can be the United States and other regions as they become available.	Standard Contractual Clauses

PART II – Palantir Affiliates

Provided that an adequate level of data protection consistent with the Data Protection Laws and this Agreement is ensured by Palantir, Customer specifically authorizes Palantir Affiliates as listed here and as updated from time to time to act as Palantir's Subprocessor(s) including by Processing Customer Personal Data for the purposes of the Agreement for the delivery of Service and/or Professional Services to Customer. Where required, Palantir and its respective Affiliate have entered into the Standard Contractual Clauses. Such Processing, where applicable, shall occur under the control and direction of Palantir and shall occur on systems managed or otherwise controlled by Palantir.

Exhibit A Updates	
24 March 2022	Addition of Microsoft Corporation and Google LLC as Third-Party Subprocessors. Authorization for subprocessing by these additional subprocessors is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
2 May 2023	Addition of the AI services to the types of purposes of using Azure. Addition of East US, South Central US, West Europe and other Azure regions as the location of the cognitive processing service. This update is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
30 May 2023	Globalization of our DPA. Amendment of our data transfers provisions to reflect latest regulatory updates. This update is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
18 August 2023	Addition of AI services to the types of purposes for using Google and AWS AI. Addition of alerting and encrypted notification services for the purpose of using AWS. This update is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
30 October 2023	Addition of OpenAI LLC as a Third-Party Subprocessor. Authorization for subprocessing by this additional subprocessor is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
22 May 2024	Addition of Oracle America, Inc. as a Third-Party Subprocessor. Authorization for subprocessing by this additional subprocessor is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.

14 January 2025	Addition of X.AI LLC as a Third-Party Subprocessor. Authorization for subprocessing by this additional Subprocessor is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
11 July 2025	Addition of Anthropic, PBC as a Third-Party Subprocessor. Authorization for subprocessing by this additional Subprocessor is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
20 November 2025	Clarification of definitions, amendment of Section 7 and the addition of DIFC SCCs to Exhibit D.

EXHIBIT B

Subject Matter and Details of Customer Personal Data Processing

Categories of Data Subject Whose Personal Data May be Subject to Processing

Data Subjects include the individuals about whom Personal Data is provided to Palantir via the Service (as applicable) or otherwise by (or at the direction of) Customer or Customer's Users.

Categories of Customer Personal Data

Customer Personal Data provided to Palantir for Processing (including via the Service) by or at the direction of Customer or Customer's Users.

Subject Matter of Processing

Palantir's provision of the Service and Professional Services and performance of its obligations under the Agreement.

Nature and Purpose of Processing

Palantir will Process Customer Personal Data in accordance with the terms of this DPA for the purpose of providing the Service and Professional Services to Customer, or as otherwise compelled by applicable law.

Duration of Processing

Continuous for duration of the Agreement, plus the period from the expiry of the Agreement until the return or deletion of all Customer Personal Data by Palantir in accordance with the Agreement (including this DPA), Customer Instructions and applicable law.

Subject matter, nature and duration of processing by sub-processors

As set out in Exhibit A. The duration of sub-processing is as set out immediately above.

EXHIBIT C – APOLLO SERVICES

The following capitalized term will have the meaning indicated below:

"**Apollo Services**" means the specific Service selected by Customer in the Order Form for end-to-end continuous deployment SaaS solution, enabling Users to centrally manage multiple versions of Palantir Technology across independent environments and as exclusively described in the present Exhibit C for Apollo Services, excluding the application of Exhibit A and Exhibit B of the present DPA;

EXHIBIT C-1

List of approved Subprocessors

PART I – Subprocessors

The following third parties are hereby specifically authorized by Customer to carry out work as Third-Party Subprocessors for purposes of providing Apollo Services to Customer under the Agreement.

Authorized Third-Party Subprocessors				
Subprocessor	**Purpose**	**Registered Address**	**Location**	**Transfer Mechanism**
Amazon Web Services, Inc.	Cloud hosting and infrastructure, alerting and encrypted notification services.	410 Terry Avenue North, Seattle, WA 98109, USA	As selected by Customer in the Order Form or, as applicable, other parts of the Agreement	Standard Contractual Clauses
Microsoft Corporation	User authentication as an identity provider (where selected as chosen identity provider by Customer).	One Microsoft Way, Redmond, WA 98052, USA	United States	Standard Contractual Clauses
Oracle America, Inc.	Cloud hosting and infrastructure.	500 Oracle Parkway, Redwood Shores, CA 94065, USA	As selected by Customer in the Order Form or, as applicable, other parts of the Agreement	Standard Contractual Clauses

PART II – Palantir Affiliates

As described under "PART II – Palantir Affiliates" in Exhibit A.

EXHIBIT C-2

Subject Matter and Details of Customer Personal Data Processing

For the provision of Apollo Services, the following shall apply:

Categories of Data Subject Whose Personal Data May be Subject to Processing

Data Subjects include the individuals about whom Personal Data is provided to Palantir via the Apollo Service or otherwise by (or at the direction of) Customer or Customer's Users.

Categories of Customer Personal Data

Customer Personal Data provided to Palantir for Processing via the Apollo Service by or at the direction of Customer or Customer's Users. Categories of Customer Personal Data include Users identification details: name, addresses, email addresses and IDs.

Subject Matter of Processing

Palantir's provision of the Apollo Service under the Agreement.

Nature and Purpose of Processing

Palantir will Process the above detailed Customer Personal Data in accordance with the terms of this DPA for the purpose of setting up Apollo Users' accounts, providing the Apollo Service to Customer including scanning managed environments for vulnerabilities, or as otherwise compelled by applicable law.

Duration of Processing

Continuous for duration of the Agreement, plus the period from the expiry of the Agreement until the return or deletion of all Customer Personal Data by Palantir in accordance with the Agreement (including this DPA), Customer Instructions and applicable law.

Subject matter, nature and duration of processing by sub-processors

As set out in Exhibit A. The duration of sub-processing is as set out immediately above.

EXHIBIT D

Additions to the Standard Contractual Clauses

The following capitalized term will have the meaning indicated below:

"**UK Addendum**" means the international data transfer addendum to the EU SCCs issued by the UK Information Commissioner under s. 119A of the Data Protection Act 2018, or such other addendum as may amend or replace the addendum from time to time.

"**DIFC SCCs**" means the Model Clauses for Data Export to importers in non-Adequate Countries as prescribed in DIFC Laws.

"Completions" means

(i) in relation to the EU SCCs in relation to exports from the EEA:

    a) the optional wording at Clauses 7 and 11 is deleted;

    b) in Clause 8.9 of such SCCs, the following paragraph is added after subsection (d):

"*(e) Notwithstanding the above, any audit will be limited in scope and parameter to the systems processing the relevant personal data.*

    Where audits include inspections, they shall be carried out with reasonable prior notice. The parties will mutually agree upon the scope, timing, duration, control and evidence requirements of the audit, provided that this requirement to agree will not permit the data importer to unreasonably delay performance of the audit.

    Any audit made pursuant to this Clause (i) shall be at the expense of the requesting data exporter, and such expenses shall include any reasonable related costs of the data importer, including compensation for the hours worked by the data importer's staff; (ii) may, if the data exporter seeks to retain an independent auditor, only be done by a party approved in advance by the data importer, which approval cannot be unreasonably withheld; and (iii) shall be subject to a non-disclosure agreement."

    c) in Clause 9, Option 1 is deleted and the time period shall be not less than 30 days;

    d) the applicable wording for Clause 13(a) of the EU SCCs (as determined by the instructions in square brackets in such SCCs) is retained and the two remaining alternatives are deleted;

    e) in Clause 17 of the EU SCCs, Option 2 is deleted and Option 1 is completed with details of the laws of Ireland and in Clause 18(b) of the EU SCCs is completed with details of the courts of Ireland;

    f) the parties set out in Annex 1 shall be completed with the names of the Customer as exporter and Palantir as importer, the transfers shall be as described in Exhibit B and any other relevant exhibits for applicable additional Services under this DPA and the supervisory authority shall be the Irish supervisory authority; in Annex II the list of technical and organisational measures

shall be the Technical and Organisational Measures and in Annex III the list of sub-processors shall be those set out in Exhibit A; and

g) in the event that the EU SCCs are replaced from those in force at the Effective Date, such completions shall be made to the revised SCCs as most closely replicate those set out above.

(ii) in relation to the EU SCCs in relation to exports from other jurisdictions besides the EEA the completions set out in (i)(a)-(g) above shall apply save that:

a) in Clause 17 of such EU SCC, the second sentence is replaced with the following: "The Parties agree that this shall be English law" save where another governing law of the EU SCCs is required as a mandatory requirement of the Data Protection Law of the relevant country, in which case Clause 17 shall be completed with details of the law which that Data Protection Law requires must be applied to such EU SCCs;

b) Clause 18(b) is replaced with the following "18(b) The Parties agree that those shall be the courts of England & Wales" save where another country, state or territory must have jurisdiction over the EU SCCs as a mandatory requirement of the Data Protection Law of the relevant country, in which case Clause 18(b) of such EU SCCs shall be completed with details of the country, state or territory which that Data Protection Law requires must have jurisdiction over the EU SCCs;

c) references in the EU SCC to "a third party located outside the European Union" are replaced by references to "a third party located outside the country or territory in which the data exporter is established";

d) references in such EU SCC to "the Member State" are replaced by references to "the country or territory in which the data exporter is established";

e) all references to the GDPR in such EU SCC are replaced by references to Data Protection Law of the relevant country and references to provisions or concepts of the GDPR are replaced by references to the provisions or concepts of such Data Protection Law most closely related to the relevant term as understood in the GDPR;

f) all references to Member States of the European Union or to the European Union are replaced by references to the country of establishment of the exporter;

g) save where required as mandatory requirement of the relevant Data Protection Law, all references in the EU SCC to (a) data subject rights or other third party beneficiary rights or (b) to obligations or liability towards data subjects or other third parties shall be deleted and ignored; and

h) to the extent that any of references to the EU SCCs referred to above under (i) to (viii) are replaced in any amended provisions or replacement or subsequently approved clauses or instrument after the Effective Date, the amendments provided above under (ii)(a)-(h) shall be adapted and/or completed if and to the extent appropriate to reflect the effect of the former as close as possible

(iii) in relation to SCCs in relation to exports from the UK the EU SCCs shall apply as amended by either (i) the Information Commissioner's "UK Addendum to the EU Commission Standard Contractual Clauses" found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdfhttps://ico.org.uk/media/about-the-ico/consultations/2620398/draft-ico-addendum-to-com-scc-20210805.pdf or (ii) such replacement addendum to the EU Standard Contractual Clauses as the Information Commissioner might issue from time to time (these addenda known as the "**UK SCC**"), with the following items completed (or in the case of (ii) those items as most closely approximate the following items):

a) to the extent not covered by the foregoing, the completions set out in (i)(a)-(g) above shall apply save that:

b) Table 1 shall be completed with the names of the Customer as exporter and Palantir as importer;

c) in Table 2 the module of the EU SCCs selected shall be determined in accordance with the definition of SCCs set out below;

d) in Table 4 the "neither party" option shall be selected,

(iv) in relation to SCCs in relation to exports from Switzerland, the EU SCCs shall apply (incorporating the completions set out at (i)(a)-(g) above), as amended by the Swiss Federal Act on Data Protection (FADP);

(v) in relation to SCCs in relation to exports from the DIFC, the EU SCCs as amended by the abbreviated DIFC SCCs found at https://edge.sitecorecloud.io/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/data-protection-pages/data-export-and-sharing/difc_abbreviated_sccs_2023.docx shall apply to any transfers from the DIFC.

a) ***Standard Contractual Clauses for Compliance with Article 27 of the Data Protection Law, DIFC Law No 5 of 2020***.

As set out in Clause 13 of the DPA regarding transfers of Personal Data to a Third Country that is not yet considered adequate by the DIFC Commissioner of Data Protection or relevant supervisory authority in the EU, the standard contractual clauses (SCCs) available at the link above are deemed to be appended to the general framework agreement and binding on the Parties in order to comply with Article 27 of the Data Protection Law, DIFC Law No 5 of 2020

DIFC SCCs:

For the purposes of Clause 9 (1)(a), the Parties agree to Option

The EU SCCs

Module 1 (Controller to Controller), Module 2 (Controller to Processor), and Module 3 (Processor to Processor), as relevant to the particular Restricted Transfer of Personal Data.

b) The parties to the SCCs shall be completed with the name of the Company as the Data Exporter and the Palantir as the Data Importer.

c) Annex 1 shall be completed as follows:

a. The Data Importer shall be a controller of any personal data relating to marketing activities that is transferred by the Data Exporter in the course of the provision of the services.
b. The Data Importer shall be the processor of any Customer Personal Data processed in the platform in the course of providing services to the Data Exporter.
c. The Data Subjects, Categories of Data being processed, and the Subject Matter and Nature of the Processing shall be as set out in Exhibit B to the DPA.

d) Annex 2 shall be completed with the details set out in Annex III of the EU SCCs set out below.

e) Annex 3 shall be completed with the details set out in Exhibit A to the DPA.

(vi) in relation to SCCs in relation to exports from any other country, the completions set out in (i)(a)-(g) above shall be made or such other Completions as most closely achieves the same outcome as those Completions.

In respect of any transfers of Personal Data that may occur in the course of the provision of the Service, Module 2 (Controller to Processor) terms, as provided below in Annex 1 to Exhibit D, shall apply to the extent Customer is a Controller of Customer Personal Data. The Module 3 (Processor to Processor) terms, as provided below in Annex 2 to Exhibit D, shall apply to the extent Customer is a Processor (or subprocessor) of Customer Personal Data. For both Module 2 and Module 3 of the Standard Contractual Clauses, the election of specific terms and/or addition of required information shall apply as follows:

(a) The applicable wording for Clause 13(a) of the Standard Contractual Clauses (as determined by the instructions in square brackets in the Standard Contractual Clauses) is retained and the two remaining alternatives are deleted;

(b) details of Subprocessors the data importer intends to engage as set out in Exhibit A and/or any other relevant exhibits for applicable additional Services, respectively, to this Agreement are the "agreed list" of Subprocessors referred to in Clause 9(a) of the Standard Contractual Clauses.