PALANTIR DATA PROTECTION ADDENDUM (“DPA”)

Version 3.0 – October 30, 2023

BY SELECTING“I AGREE” (OR EQUIVALENT) WHERESUCH OPTION ISMADE AVAILABLE, ORBY INSTALLING, EXECUTING,DOWNLOADING, ACCESSING OROTHERWISE USING ANYPORTION OF THEPALANTIR TECHNOLOGY (AS DEFINED IN THE AGREEMENT), YOUCONFIRM THAT YOU (“YOU” OR “YOUR” OR “PERMITTED USER”) HAVEREAD THIS DPA, THATYOU UNDERSTAND THE TERMS OF THIS DPA, AND THAT YOU AND (IF APPLICABLE) THE ENTITY THAT YOU REPRESENT ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS DPA. IF YOU ARE ENTERING INTO THIS DPA ON BEHALF OF AN ENTITY, SUCH AS THE COMPANY, ORGANIZATION, OR EDUCATIONAL INSTITUTION FOR WHICH YOU WORK, YOU REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO ACCEPT THE TERMS OF THIS DPA ON BEHALF OF THE ENTITY AS ITS AUTHORIZED LEGAL REPRESENTATIVE. IF YOU DO NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS DPA, DO NOT SELECT "I AGREE” (OR EQUIVALENT) WHERE SUCH OPTION IS MADE AVAILABLE AND DO NOT INSTALL, EXECUTE, DOWNLOAD, ACCESS, OR OTHERWISE USE ANY PORTION OF THE PALANTIR TECHNOLOGY.

PALANTIR’S ACCEPTANCE IS EXPRESSLY CONDITIONED UPON YOUR ASSENT TO ALL THE TERMS AND CONDITIONS OF THIS DPA, TO THE EXCLUSION OF ALL OTHER TERMS; IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS.

Customer and Palantir (as defined in the Agreement; each of Customer and Palantir a “**Party**” and collectively the “**Parties**”), have entered into an agreement (Palantir Terms of Service) 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**”).

1 DEFINITIONS

Capitalized terms used but not defined in this DPA shall have the meanings provided in the Agreement. 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 in respect of Customer, any of Customer’s affiliate(s) from time to time which are subject to Data Protection Laws and are permitted to use the Services pursuant to the Terms of Service between Customer and Palantir, but are not a party to the Terms of Service and shall include, without being limited to, all entities listed in Exhibit A, Part II, of the present DPA, and, in respect of Palantir, any Palantir’s affiliates from time to time;

- "**Completions**" has the meaning given to it in Exhibit C 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 "business" under applicable Data Protection Laws;
- "**Country**" means a country, state, province, territory or economic union that have implemented 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 of Palantir's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized use, disclosure of, or access to, Customer Personal Data on systems managed or otherwise controlled by Palantir;
- "**Data Protection Authority**" means, an independent public authority responsible for monitoring the application of Data Protection Laws;
- "**Data Protection Laws**" means all laws and regulations as amended from time to time regarding data protection, privacy, electronic communications and marketing laws to the extent applicable to the Processing of Customer Personal Data by Palantir under the Agreement;
- "**Data Protection Officer**" means the natural person or company appointed where necessary under applicable Data Protection Laws;
- "**Data Subject**" means the identified or identifiable person to whom Personal Data relates;
- "**Europe**" means the European Union, the European Economic Area, Switzerland and the United Kingdom ("**UK**") and "**European**" shall have the equivalent related meaning;
- "**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;
- **"GDPR"** means, as applicable, 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 ("**EU GDPR**") and/or the EU GDPR as implemented or amended in the United Kingdom ("**UK GDPR**");
- "**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 as personal data, personal information, 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;
- "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable the term "service provider" and any equivalent or similar terms that address the same responsibilities under applicable 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) in the absence of the Standard Contractual Clauses to be established under Section 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**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data to a third party for valuable consideration;
- **"Share"** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data to a third party for cross-context behavioral advertising;
- "**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, including the EU SCCs in relation to exports of personal data from the EEA (and where more than one set of such clauses has been approved, those that most closely approximate the EU SCCs); 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, 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;
- "**Sub-Processor**" means a provider of third party Services, or Palantir's Affiliate engaged by or on behalf of Palantir to Process Customer Personal Data in connection with the Agreement; 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 Data Protection Laws.

2 TERM

This DPA will take effect from the Effective Date of the Agreement 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

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 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 in this DPA shall prevail and control.

4 ROLES OF THE PARTIES

Customer, and any relevant Customer Affiliate, hereby appoints Palantir as a Processor or Sub-Processor, as applicable, of the Customer Personal Data. Customer shall be liable and responsible as the Controller (or Processor, if Customer is processing as a Processor any personal data forming part of the Customer Personal Data) and Palantir shall be the Processor (or Sub-Processor), in respect of Customer Personal Data. The subject matter and details of processing are as described in the Agreement and this DPA, including Exhibit B (subject matter and details of Customer Personal Data processing). In the event that Customer acts as a Processor (or Sub-Processor) 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 on behalf of the Controller in relation to Customer Personal Data. Both Parties shall comply with applicable Data Protection Laws as relevant to their respective Processing of Personal Data under the Agreement.

5 CUSTOMER PROCESSING OF PERSONAL DATA

5.1 Customer shall ensure that any processing of Personal Data carried out by Palantir consistent with Customer's instruction, which shall include Customer's use of the Service, shall comply with all applicable Data Protections Laws. Customer instructs Palantir to Process Customer Personal Data: (a) to provide the Service specified in the Agreement and Documentation and 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 documented in any other written instructions given by Customer in writing and acknowledged in writing by Palantir 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 to the Customer by Palantir, which shall be payable in accordance with the terms of the Agreement.

5.2 Customer shall have sole responsibility for 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 any 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, authorisations, approvals, and/or agreements (including, where Customer is a Processor or Sub-Processor, with and from the applicable Controller(s)) and provided Data Subjects with any option required under applicable Data Protection 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, and may only include government related identifiers (where that term is defined under applicable Data Protection Laws) in the Customer Personal Data to the extent that the Processing of such government related identifiers are permitted under applicable Data Protection Laws.

6 PALANTIR PROCESSING OF PERSONAL DATA

Palantir will process Customer Personal Data for the purposes of performing the services and this DPA unless set out in this clause, or

the processing is required by applicable law to which Palantir is subject, in which case Palantir shall to the extent permitted by applicable laws inform the Customer of that legal requirement before the relevant Processing of that personal data. 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 it pertains 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 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 the Processing occurs unless legally prohibited from doing so;

(c) 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 that Palantir may combine Customer Personal Data as necessary to perform its internal business purposes that do not involve combining Customer Personal Data for interest-based advertising;

(d) ensure that all persons authorized by Palantir to Process Customer Personal Data, including any Sub-Processors, 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; and

(e) take reasonable steps to destroy Customer Personal Data or ensure that Customer Personal Data is de-identified when it is no longer necessary for the purposes of performing the relevant Services upon the termination of the Agreement, and the obligations under this DPA, where required under applicable Data Protection Laws.

7 SUB-PROCESSORS

7.1 Customer specifically authorizes the engagement of, as Sub-Processors, the entities listed in Exhibit A hereto provided that, prior to permitting such Sub-Processors to Process any Customer Personal Data, Palantir shall enter into a written agreement with the Sub-Processor imposing terms that are no less restrictive than those set out in this DPA or otherwise sufficient to meet the requirements of Data Protection Laws.

7.2 Subject to Section 7.3, Customer generally authorizes Palantir to engage additional Sub-Processors ("Additional Sub-Processors"), provided that, prior to permitting any such Additional Sub- Processor to Process any Customer Personal Data, Palantir shall enter into a written agreement with the Additional Sub-Processor imposing terms that are consistent with those set out in this DPA or otherwise sufficient to meet the requirements of Data Protection Laws.

7.3 Should Palantir engage an Additional Sub-Processor, it shall provide Customer with no less than 30 days' notice, including the identity, location, and nature of Processing proposed to be undertaken by such Additional Sub-Processor. That notice may be given by any typical means Palantir uses to communicate with the Customer from time to time. Where Customer indicates in writing that it objects to the Processing of Customer Personal Data by such Additional Sub-Processor, the Parties shall seek to resolve the Customer concerns, and where necessary the Customer may exercise its applicable rights to terminate the Agreement.

7.4 To the extent required by Data Protection Law, Palantir shall remain liable to Customer for the performance of the Sub-Processors' obligations in relation to this Section 7 ("Sub-Processor 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 Sub-Processor Data Protection Liability.

8 SECURITY

8.1 Palantir shall take the Technical and Organisational Measures to protect the confidentiality, integrity, availability and resilience of Palantir's systems Processing Personal Data. Palantir may update the Technical and Organisational Measures from time to time provided that any such updates are no less protective than the original Technical and Organisational Measures.

8.1 The 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 the Customer to Palantir or made available by Customer to Palantir in relation to the Services and Professional 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.

8.3 Palantir shall assist the Customer to comply with its own data security obligations under Data Protection Laws where required by the Customer in writing. If and to the extent that:

(a) such assistance requires Palantir to take additional steps beyond those imposed on Palantir by Data Protection Laws or required pursuant to the Agreement; or

(b) the relevant actions required pursuant to Section 8.3 are required as a result of an act or omission by the Customer or a party acting on behalf of the Customer in breach of this Agreement or Data Protection Laws,

then Palantir's obligation to provide its assistance shall be subject to the Customer's payment of Palantir's reasonable fees in respect of such additional assistance.

9 AUDIT

9.1 Palantir uses third party auditors to verify the adequacy of its security measures.This audit is performed at least annually, by independent third-party auditors at Palantir's selection and expense, 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").

9.2 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 so that Customer can reasonably verify Palantir's compliance with the data security and data protection obligations under this DPA. Subject to Section 9.3, if Data Protection Laws, Standard Contractual Clauses, or the Agreement require Palantir to provide Customer with access to Palantir facilities or information in addition to the Report and the Accountability Information, then Palantir shall permit Customer to audit 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.

9.3 In order to request an audit of Palantir's facilities under this Section 9 Customer shall notify Palantir and the Parties shall agree, as soon as reasonably possible but always in advance, the reasonable dates, duration and scope of the audit, the identity and qualifications of the auditor and any security and confidentiality controls required for access to the information or Processes in scope of such audit. Palantir may object to any external auditor if, in Palantir's reasonable opinion, the auditor is not qualified, does not have appropriate security controls to ensure Palantir's Confidential Information is suitably protected, is a competitor to Palantir or its suppliers, or is not independent. If Palantir objects to the identity or qualifications of any proposed auditor, Palantir shall provide reasons for such objection and Customer will be required to propose an alternate auditor. The scope of any audit under this Section 9 shall be limited to Palantir systems and facilities used to Process Customer Personal Data and Documentation directly related to such Processing. The Customer shall bear the reasonable costs of Palantir in fulfilling any requirements under this Section.

9.4 All information provided or made available to Customer or its auditor pursuant to this Section 9 shall be Confidential Information of Palantir.

9.5 In the event of any confirmed non-compliance by Palantir with the terms of this DPA, Customer may take reasonable steps to remediate the same, without prejudice to any contractual and legal obligations contained in the Agreement and this DPA. 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.

10 DEALINGS WITH DATA PROTECTION AUTHORITIES AND DATA PROTECTION IMPACT ASSESSMENTS

10.1 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.

10.2 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 and prior consultation where applicable under Data Protection Laws, by providing the Report, Accountability Information and Documentation.

11 ACCOUNTABILITY

11.1 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 Sub-Processors;

(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**".

12 DATA SUBJECT RIGHTS

12.1 Where Palantir directly receives requests from any Data Subjects, or anyone acting on their behalf, to exercise their rights under Data Protection Laws, including to withdraw any consent ("Data Subject Request"), or to make 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.

12.2 The Service provides Customer with controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data (including Customer Personal Data) as described in the Documentation. Customer may use these controls as technical and organisational measures to assist it in connection with its obligations under Data Protection Laws, including its obligations relating to responding to requests from Data Subjects. Where such controls are not sufficient to assist Customer in responding to requests from Data Subjects, Palantir shall, upon reasonable request and at Customer's cost, use reasonable endeavours to assist the Customer (insofar as possible) with the Customer's obligation to respond to requests from Data Subjects.

13 DATA INCIDENT

13.1 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 Sub-Processor; 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.

13.2 Any information provided by Palantir pursuant to this Section 13 shall be the Confidential Information of Palantir and Palantir's notification of or response to a Data Incident under this Section 13 will not be construed as an acknowledgement by Palantir or, if relevant, its Sub-Processors of any fault or liability with respect to the performance of any Service or Professional Services (as applicable).

14 DATA TRANSFERS

14.1 Palantir may Process Customer Personal Data in countries outside of the Country in which Customer is established in which Palantir or its Sub-Processors maintains facilities or infrastructure.

14.2 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 has implemented Data Protection Laws to Palantir (or anyPalantir Affiliate) in any country that is not deemed to be an Adequate Country, then:

(a) the Parties shall hereby enter into a set of SCCs; and

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

(c) Palantir shall ensure that transfers of Personal Data between Palantir and any Palantir third party Sub-Processors, are subject to contractual terms between Palantir and the relevant third party Sub-Processor providing appropriate safeguards and containing clauses equivalent to the SCCs.

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

15 LIABILITY

15.1 Subject to 15.2 and 15.3, 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.

15.2 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.

15.3 Customer shall ensure that all Customer Data it uploads onto Palantir platforms is accurate and complies with all applicable laws. Palantir does not monitor or control any Customer Data on Palantir platforms, and 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 this clause or any applicable laws in connection with Customer Data.

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, if this is not possible, (ii) construed in a manner as if the invalid off unenforceable part had never been contained therein.

16.2 Palantir may notify the 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. Any such changes required shall take effect on the date falling 25 working days after the date such written notice is sent by Palantir to the Customer.

17 GOVERNING LAW AND JURISDICTION

17.1 Palantir may modify the terms of this DPA by not less than 30 days' notice to the Customer, using the correspondence method typically used by Palantir to communicate with its customers, if such modification is required for either or both of 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. In all other circumstances, the Parties may amend this DPA by agreement in writing.

17.2 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, to the extent required to satisfy such laws.

17.3 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. 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.

EXHIBIT A

LIST OF APPROVED SUB-PROCESSORS

Part I – Sub-Processors

To perform its obligations under the Agreement and this DPA, Palantir and its Affiliates may use third-party data Sub-Processors ("**Third-Party Sub-Processors**") and Palantir Affiliates to process Customer Personal Data.

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

Authorized Third-Party Sub-Processors				
Sub-Processor	**Purpose**	**Registered Address**	**Location**	**Transfer Mechanism**
Amazon Web Services, Inc.	Cloud hosting, infrastructure, AI services and alerting and encrypted notification	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, 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 of providing the AI service is East US, South Central US, West Europe and/or other Microsoft Azure regions as they become available.	Standard Contractual Clauses
Google LLC	Cloud hosting, infrastructure and AI services (Google Cloud Platform)	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	Standard Contractual Clauses

			the AI services are all regions available for features of Generative AI on Google Vertex AI and other regions as they become available.	
Proofpoint, Inc.	Alerting and encrypted notification service	892 Ross Drive, Sunnyvale, CA 94089, 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
OpenAI LLC	AI services	3180 18th Street, San Francisco, CA 94110, USA	The location for the purpose of providing the AI services can be the United States and other regions as they become available.	Standard Contractual Clauses

PART II – Palantir Affiliates

Customer specifically authorizes Palantir Affiliates as listed here and as updated from time to time to act as Palantir's Sub-Processor(s) including by Processing Customer Personal Data for the purposes of the Agreement for the delivery of Service and/or Professional Services to Customer. 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

29 August 2023	Addition of alerting and encrypted notification services for the purpose of using AWS. This update is considered effective or 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.

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 pursuant to the Agreement, 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.

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

As set out in the Agreement. The duration of sub-processing is as set out immediately above.

EXHIBIT C

Definition of Completions

"**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 [31] 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 the supervisory authority shall 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)-(g) 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 either (a) the FDPIC' decision guidance of 27 August 2021 found at https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-1259254222 setting out amendments to be made to the EU SCCs in respect of transfers subject to the Swiss FADP or (b) such replacement decision of the FDPIC relating to amendments to be made to the EU SCCs from time to time (these amendments known as the "**Swiss SCCs**");

(v) in relation to SCCs in relation to exports from Canada:

a) the rights and obligations of the EU SCCs for the protection of the Personal Data of European individuals will apply *mutatis mutandis* to the protection of the Personal Data of Canadian individuals; and

b) the terms and conditions in place between Palantir and its Sub-Processors for the protection of the Personal Data of European individuals will apply *mutatis mutandis* to the protection of the Personal Data of Canadian individuals when their Personal Data is transferred outside of Québec.

(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.