PALANTIR DATA PROTECTION ADDENDUM

(“DPA”)

Last modified: August 26, 2021

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 and Conditions of Access and Order Form) governing Customer’s use of Palantir Products and provision of related 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 or territory outside of the EEA that the European Commission has deemed to provide an adequate level of protection for Personal Data pursuant to a decision made in accordance with Article 45(1) of the EU GDPR, or country or territory having equivalent status under the UK GDPR (as applicable);
- “**Affiliates**” means any other entity that directly or indirectly controls, is controlled by, or is under common control with a Party;
- “**Customer Personal Data**” means any Personal Data contained within Content subject to Data Protection Laws that Customer, including Authorized Users, provides or makes available to Palantir in connection with the Agreement;
- “**Data Protection Laws**” means all laws and regulations regarding data protection and privacy to the extent applicable to the Processing of Customer Personal Data by Palantir under the Agreement, such as:
    - California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (“**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**”);
    - The EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 (“**UK GDPR**”); and
    - The Switzerland Federal Data Protection act of 19 June 1992 as replaced and/or updated from time to time (“**FDP**”).
- “**Data Incident**” means any breach 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.
- “**DPA Effective Date”** means the Effective Date of the Agreement.
- “**EEA**” means the European Economic Area.
- “**European Data Protection Law”** means, as applicable, the GDPR and/or the FDP.
- “**GDPR**” means, as applicable, the EU GDPR and/or the UK GDPR.
- “**International Transfer Solution”** means appropriate safeguards established by Palantir in relation to the transfer of Personal Data from the EEA or the UK to a country or territory outside of the EEA or the UK (respectively) that is not an Adequate Country (a “**Third Country**”) in accordance with Article 46 of the GDPR.

- "**Security Documentation**" means the Documentation describing the security standards that apply to the Products and Services (as applicable) as provided by or on behalf of Palantir from time to time.
- "**Sell**" has the meaning set forth in the CCPA, Cal. Civ. Code § 1798.100 et seq.
- "**Subprocessor**" means a third party engaged by or on behalf of Palantir to Process Customer Personal Data in connection with the Agreement.
- "**Supervisory Authority**" means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR.
- "**Standard Contractual Clauses**" means the standard data protection clauses for the transfer of Personal Data from Controllers (or Processors, as applicable) established inside the EEA or the UK to Processors established in Third Countries, as adopted by the European Commission from time to time and incorporated by reference (in the case of transfers from the EEA) or approved by the Information Commissioner's Office from time to time and incorporated by reference (in the case of transfers from the UK), in each case with the inclusions specified in Exhibit C made in the specified locations in the clauses approved by European Commission implementing decision 2021/914 (or where alternative clauses are the Standard Contractual Clauses, inclusions in the locations that are most closely equivalent to those listed below, and such other inclusions as are necessary to give effect to the alternative clauses in such manner as is most closely equivalent to the clauses in implementing decision 2021/914).
- "**UK**" means the United Kingdom.

1.2 The terms "**Personal Data**", "**Process**" (and its derivatives being construed accordingly), "**Controller**", "**Processor**", "**Representative**", "**Data Protection Officer**", "**Data Subject**" and "**Consent**" shall each have the meanings as set out in the GDPR.

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. APPLICATION OF DATA PROTECTION LAWS

3.1 Except to the extent this DPA specifies otherwise, the terms of this DPA shall apply to the Processing of Customer Personal Data whether or not European Data Protection Law applies.

3.2 The Parties agree that European Data Protection Law will apply to the Processing of Customer Personal Data including to the extent that:

(a) the Processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA and/or the UK; and/or

(b) the Customer Personal Data relates to Data Subjects who are in the EEA and/or the UK and the Processing relates to the offering to them of goods or services in the EEA and/or the UK, or the monitoring of their behavior in the EEA and/or the UK.

3.3 Subject to Section 4.5, if Data Protection Laws other than European Data Protection Laws apply to the Processing of Customer Personal Data hereunder, Customer shall ensure that Customer Instructions identify, and are in accordance with, and the Parties will comply with, the requirements applicable under such Data Protection Laws.

4. CONTROLLER AND PROCESSOR OBLIGATIONS

4.1 As between the Parties, Customer shall be liable and responsible as the Controller (or Processor, if Customer is Processing third party Personal Data with the Palantir Products) and Palantir shall be liable and responsible as the Processor (or Subprocessor), 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 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. The Products and Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Content (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.

4.2 Customer instructs Palantir to Process Customer Personal Data: (a) to provide the Products and Services specified in the Agreement and Documentation or otherwise perform its obligations thereunder; (b) as further initiated by Customer via Customer's or Authorized Users use of the Products and Services in accordance with the Agreement and Documentation; and/or (c) for 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 as constituting instructions for purposes of this DPA (collectively, "Customer Instructions"). Customer Instructions which have a material impact on the cost and/or structure of the provision of the Products and/or Services shall be set out in the Agreement. Customer may elect to implement certain technical and organisational measures in relation to Content (including Customer Personal Data) Processed via the Products as described in the Documentation.

4.3 Palantir shall:

(a) designate and maintain a Data Protection Officer and a data protection team that meets the requirements of the GDPR as it pertains to Processors, which can be contacted at privacy@palantir.com;

(b) not Sell Customer Personal Data or otherwise Process Customer Personal Data for any purpose other than for the fulfillment 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) 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; and

(d) 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.

4.4 Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data, the means by which it acquires and uses Customer Personal Data, and for Customer Instructions regarding the Processing of Customer Personal Data. Customer represents and warrants that it has provided (or procured the provision of) all notifications and obtained (or procured the provision of) all consents (including Consents), authorisations, 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.

4.5 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.

5. SUBPROCESSORS

5.1 Customer specifically authorizes the engagement as Subprocessors of (a) the entities listed in Exhibit A hereto; and (b) all Palantir Affiliates from time to time, provided that, prior to permitting such Subprocessors to Process any Customer Personal Data, Palantir shall enter into a written agreement with the Subprocessor imposing terms that are consistent with those set out in this DPA or otherwise sufficient to meet the requirements of Data Protection Laws.

5.2 Subject to Section 5.3, Customer generally authorizes Palantir to engage additional Subprocessors ("**Additional Subprocessors**"), provided that, prior to permitting such Additional Subprocessor to Process any Customer Personal Data, Palantir shall enter into a written agreement with the Additional Subprocessor imposing terms that are consistent with those set out in this DPA or otherwise sufficient to meet the requirements of Data Protection Laws.

5.3 Should Palantir engage an Additional Subprocessor, 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 Subprocessor. Customer may, within 60 days

of such notification, object to Processing of Customer Personal Data by such Additional Subprocessor by providing written notice to Palantir.

5.4 To the extent required by Data Protection Law, Palantir shall remain liable to Customer for the performance of the Subprocessor's obligations in relation to this Section 5 ("**Subprocessor Data Protection Liability**"), and 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.

6. AUDIT

6.1 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 according to 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. Palantir's Products 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").

6.2 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 outlined in Section 7 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 6.3, 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.

6.3 In order to request an audit of Palantir's facilities under this Section 6 (and where such an audit is authorized), 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, the costs, 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 6 shall be limited to Palantir systems and facilities used to Process Customer Personal Data and Documentation directly related to such Processing.

6.4 All information provided or made available to Customer pursuant to this Section 6 shall be Confidential Information of Palantir.

7. DEALINGS WITH SUPERVISORY AUTHORITIES AND DATA PROTECTION IMPACT ASSESSMENTS

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

7.2 Taking into account the nature of the Products and Services 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 pursuant to Articles 35 and 36 of the GDPR, by providing the Report, Accountability Information and Documentation.

8. ACCOUNTABILITY

8.1 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**".

8.2 On reasonable written request from Customer, Palantir shall provide the Accountability Information to Customer. Such records shall be Confidential Information of Palantir.

9. DATA SUBJECT RIGHTS

9.1 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.

9.2 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 Sections 4.1, 4.2, and the Documentation that Customer may elect to use to comply with its obligations towards Data Subjects.

10. DATA INCIDENT

10.1 Palantir shall notify Customer without undue delay after becoming aware of a Data Incident. 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.

10.2 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.

10.3 Any information provided by Palantir pursuant to this Section 10 shall be the Confidential Information of Palantir and Palantir's notification of or response to a Data Incident under this Section 10 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 Products and Services (as applicable).

11. DATA TRANSFERS

11.1 Palantir may Process Customer Personal Data in countries outside of the EEA in which Palantir or its Subprocessors maintains facilities or infrastructure.

11.2 Unless clause 11.3 applies, if the Processing of Customer Personal Data involves transfers of Customer Personal Data by or on behalf of Customer from the EEA, Switzerland or the UK to Palantir (or any other Palantir Technologies entity) in any Third Country, and European Data Protection Law applies to such transfers, then the transfers will be subject to the Standard Contractual Clauses between Customer and Palantir (which Standard Contractual Clauses are hereby incorporated into this DPA as further specified in Exhibit C) and Palantir will comply with its obligations as an importer under those clauses in respect of those transfers, provided that when Palantir does have an International Transfer Solution in place, such Standard Contractual Clauses shall automatically terminate. In the event of a conflict between the Agreement, this DPA, and the Standard Contractual Clauses, the latter in each case shall prevail.

11.3 If the Processing of Customer Personal Data involves transfers of Customer Personal Data by or on behalf of Palantir from the EEA, Switzerland or the UK to any Third Country, and European Data Protection Law applies to such transfers, then Palantir shall ensure an International Transfer Solution is put in place in respect of such transfer.

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

12. LIABILITY

12.1 Subject to 12.2, 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.

12.2 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.

13. GOVERNING LAW AND JURISDICTION

13.1 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

13.2 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; and/or (b) the laws of the United Kingdom, this DPA shall be governed by and construed in accordance with the laws of England and Wales, to the extent required to satisfy such laws.

EXHIBIT A

LIST OF APPROVED SUBPROCESSORS

PART I – Third-Party Subprocessors

The following companies are hereby specifically authorized by Customer to carry out work as Palantir's Subprocessor for purposes of the Agreement.

Name	Registered Address	Description of processing
Amazon Web Services, Inc. (AWS)	410 Terry Avenue North, Seattle, WA 98109	AWS provides the cloud infrastructure for Palantir products. Additional details are provided in the Documentation.
Proofpoint, Inc.	892 Ross Drive, Sunnyvale, CA 94089, USA	Proofpoint supports the alerting and encrypted notification service in Palantir products. Additional details are provided in the Documentation.

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: https://www.palantir.com/data-protection/agreement/affiliates/ (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 Products and/or 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 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 Products and Services (as applicable) or otherwise by (or at the direction of) Customer or Customer's Authorized Users.

Categories of Customer Personal Data

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

Subject Matter of Processing

Palantir's provision of the Products and 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 Products and Services to Customer, or as otherwise compelled by applicable law.

Duration of Processing

The 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, 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

Additions to the Standard Contractual Clauses

(a) the details of the Data Exporter and the supervisory authority of the Data Exporter inserted to complete Annex I.A and C of such clauses, and in addition in Annex I.A the "Activities relevant to the data transferred under these Clauses" listed as "customer under the Agreement" and the "Role" listed as controller or processor as the case maybe, as set out in the Agreement;

(b) Palantir's details are inserted from the Agreement as Data Importer to complete Annex I.A of such clauses, and in addition in Annex I.A the "Activities relevant to the data transferred under these Clauses" listed as "supplier under the Agreement" and the "Role" listed as "processor";

(c) the details of the data transfer are inserted from Exhibit B to complete Annex I.B of such clauses;

(d) the details of the technical and organisational measures described in Clause 4.3(c) inserted to complete Annex II of such clauses;

(e) details of sub-processors the Data Importer intends to engage as set out in Exhibit A to this Agreement are the "agreed list" of sub-processors referred to in Clause 9(a) of such clauses;

(f) in Clause 9(a) of such clauses, Option 1 is deleted and the time period shall be not less than 14 days;

(g) the optional wording at Clause 11(a) of such clauses is deleted;

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

(i) in Clause 17 of such clauses, Option 2 is deleted and Option 1 is completed with details of "Ireland"; and

(j) Clause 18(b) of such clauses is completed with details of the courts of Ireland.