APPENDIX B: DATA PROTECTION ADDENDUM ("DPA")

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 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:
  - 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 Swiss Federal Act on Data Protection 1992 as amended or updated from time to time ("**FADP**").
- "**Data Incident**" means any breach of Palantir's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised 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 FADP.
- "**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 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.
- "**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 described in Article 46 of the EU GDPR, forming part of this DPA and attached in Exhibit C.
- "**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. Controller and Processor Obligations

3.1. As between the Parties, Customer shall be liable and responsible as the Controller and Palantir shall be liable and responsible as the 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 Subprocessor) in respect of Customer Personal Data, Customer represents and warrants to Palantir that it is validly authorised by the relevant Controller to enter into this DPA and to provide Customer Instructions (as defined below) on behalf of the Controller in relation to Customer Personal Data and, where applicable, enter into the Standard Contractual Clauses on behalf of the Controller. 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.

3.2. 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 specified via Customer's use of the Products and Services; and/or (c) 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.

3.3 **Palantir shall:** 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 [redacted];not 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 legally binding 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;

a) *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, unauthorised 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*
b) *ensure that all persons authorised 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.*

3.4 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 all notifications and obtained all consents (including Consents), authorisations, approvals, and/or agreements 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.

3.5 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.

4. Subprocessors

4.1 Customer specifically authorises the engagement as Subprocessors of the entities listed in Exhibit A hereto.

4.2 Subject to Section 4.3, Customer generally authorises 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 and otherwise sufficient to meet the requirements of Data Protection Laws.

4.3 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.

4.4 To the extent provided for by Data Protection Laws, Palantir shall remain liable to Customer for the performance of the Subprocessor's obligations in relation to this Section 4 ("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 may diminish any claim that Customer has against Palantir in respect of any Subprocessor Data Protection Liability.

5. Audit

5.1 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").

5.2 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 5.3, 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.

5.3 In order to request an audit of Palantir's facilities under this Section 5 (and where such an audit is authorised), 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 5 shall be limited to Palantir systems and facilities used to Process Customer Personal Data and Documentation directly related to such Processing.

5.4 All information provided or made available to Customer pursuant to this Section 5 shall be Confidential Information of Palantir (subject to the general exceptions to the definition of Confidential Information within the Agreement).

6. Dealings with supervisory authorities and data protection impact assessments

6.1 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.

6.2 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.

7. Accountability

7.1 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".

7.2 On reasonable written request from Customer, Palantir shall provide the Accountability Information to Customer. Such records shall be Confidential Information of Palantir (subject to the general exceptions to the definition of Confidential Information within the Agreement).

8. Data subject Rights

8.1 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.

8.2 On reasonable written request from Customer, and taking into account the nature of the Processing, Palantir shall use commercially reasonable efforts to offer Customer certain controls as described in Sections 2.1, 3.2, and the Documentation that Customer may elect to use to comply with its obligations towards Data Subjects.

9. Data Incident

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

9.2 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.

9.3 Any information provided by Palantir pursuant to this Section 9 shall be the Confidential Information of Palantir (subject to the general exceptions to the definition of Confidential Information within the Agreement) and Palantir's notification of or response to a Data Incident under this Section 9 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).

10. Data transfers

10.1 If the Processing of Customer Personal Data involves transfers of Customer Personal Data from the UK to any Third Country, and European Data Protection Law applies to such transfers, then the transfers will be subject to the Standard Contractual Clauses and Palantir will comply with its obligations as an importer in respect of those transfers, provided that when Palantir does have an International Transfer Solution in place (other than the Standard Contractual Clauses), approved in writing by the data exporter, 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.

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

11. Liability

11.1 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.

EXHIBIT A

LIST OF APPROVED SUBPROCESSORS

Third-Party Subprocessors

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

Name	Registered Address	Description of processing
[redacted]	[redacted]	Hosting of the Software will be solely in the UK region. [redacted] provides the cloud infrastructure for Palantir products. Additional details are provided in the Documentation.
[redacted]	[redacted]	[redacted] supports the alerting and encrypted notification service in Palantir products. Additional details are provided in the Documentation.
[redacted]	[redacted]	Support services.

EXHIBIT B

Subject Matter and Details of Customer Personal Data Processing

Subject Matter of Processing

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

Duration of Processing

The Order Term, plus the period from the expiry of the Order Form until the return or deletion of all Customer Personal Data by Palantir in accordance with the Agreement, this DPA, Customer Instructions and applicable law.

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.

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 Authorised Users.

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 Authorised Users.

EXHIBIT C

STANDARD EU CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

The entity identified as "Customer" in the DPA, on behalf of itself and (as applicable):

(a) as an agent for and on behalf of all legal entities it directly or indirectly controls located inside of the European Economic Area and/or the UK (as applicable), and which from time to time serve as data controller(s) in respect of the personal data processed by or on behalf of the data exporter;

(b) in the event that Customer acts as a processor (or subprocessor) in respect of the personal data processed by or on behalf of the data exporter, as an agent for and on behalf of the relevant data controller(s).

(the "**data exporter"**)

And
Name of the data importing organisation:

Palantir Technologies Inc.

Address: 1555 Blake Street, Suite 250, Denver, CO 80202
(the "**data importer**")

Palantir Technologies UK, Ltd. enters into the Clauses as agent for and on behalf of Palantir Technologies Inc. (the data importer).

each a "**party**"; together the "**parties**",

HAVE AGREED on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been

notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the relevant data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the relevant data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the relevant data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of a data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter

The Data Exporter is the entity identified as "Customer" in the DPA, on behalf of itself and (as applicable):

(a) as an agent for and on behalf of all legal entities it directly or indirectly controls located inside of the European Economic Area and/or the UK (as applicable), and which from time to time serve as data controller(s) in respect of the personal data processed by or on behalf of the data exporter;

(b) in the event that Customer acts as a processor (or subprocessor) in respect of the personal data processed by or on behalf of the data exporter, as an agent for and on behalf of the relevant data controller(s).

Data Importer

The Data Importer is Palantir Technologies Inc., a software company. Under the Agreement, Palantir Technologies UK, Ltd. enters into the Clauses as agent for and on behalf of Palantir Technologies Inc..

Types and Categories of Personal Data Subject to Transfer

The types and categories of Personal Data and Data Subjects under these Clauses are those contained in Security Logs (as defined in the Agreement) as required for security purposes.

Processing operations (including the nature, duration and purpose of the Processing)

The data importer retains Security Logs solely for ensuring the security of the Products (as defined in the Agreement).