PALANTIR DATA PROTECTION ADDENDUM ("DPA")

BY SELECTING "I AGREE" (OR EQUIVALENT) WHERE SUCH OPTION IS MADE AVAILABLE, OR BY INSTALLING, EXECUTING, DOWNLOADING, ACCESSING OR OTHERWISE USING ANY PORTION OF THE PALANTIR TECHNOLOGY (AS DEFINED IN THE AGREEMENT), YOU CONFIRM THAT YOU ("YOU" OR "YOUR" OR "PERMITTED USER") HAVE READ THIS DPA, THAT YOU 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.

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

1 DEFINITIONS

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

- "**Adequate Country**" means a country that may import Personal Data and is deemed by the governing authority of the exporting country to provide an adequate level of data protection under the applicable Data Protection Laws;
- "**Affiliate**" means an entity that, directly or indirectly, owns or controls or is owned or controlled by, or is under common ownership or control with, a Party. As used herein, "control" means the power to direct, directly or indirectly, the management or affairs of an entity and "ownership" means the beneficial ownership of more than fifty percent of the voting equity securities or other equivalent voting interests of an entity. In respect of Palantir, Affiliate shall include, without being limited to, all entities listed in Exhibit A, Part II and any other Palantir affiliates from time to time;
- "**Completions**" has the meaning given to it in Exhibit D of this DPA;
- "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data and includes, as applicable, the term "controller" "business" and any other similar or equivalent terms under applicable Data Protection Laws;
- "**Customer Personal Data**" means any Personal Data contained within Customer Data subject to Data Protection Laws that

Customer, including Users, provides or makes available to Palantir in connection with the Agreement;

- "**Data Incident**" means any breach, as defined by applicable Data Protection Laws, of Palantir's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data on systems managed or otherwise controlled by Palantir;
- "**Data Protection Authority**" means a competent authority responsible for enforcing the application of the relevant Data Protection Laws, and includes, as applicable, any data protection authority, privacy regulator, supervisory authority, Attorney General, state privacy agency or any governmental body or agency enforcing Data Protection Laws;
- "**Data Protection Laws**" means all laws and regulations as amended from time to time regarding data protection, consumer privacy, electronic communications and marketing laws to the extent applicable to the Processing of Customer Personal Data by Palantir under the Agreement, such as:
    - California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**");
    - California Privacy Rights Act of 2020 ("**CPRA**");
    - 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 Protection Officer**" means the natural person or company appointed where necessary under applicable Data Protection Laws to ensure an organization's compliance with Data Protection Laws and cooperate with the Data Protection Authorities;
- "**Data Subject**" means the identified or identifiable person to whom Personal Data relates, and includes, as applicable, the term "consumer" and any other similar or equivalent terms under Applicable Data Protection Laws;
- "**DPA Effective Date**" means the Effective Date of the Agreement;
- "**EEA**" means the European Economic Area;
- "**EU SCCs**" means the standard contractual clauses for use in relation to exports of Personal Data from the EEA approved by the European Commission under Commission Implementing Decision 2021/914, or such other clauses as replace them from time to time;
- "**Personal Data**" means: (a) any information relating to (i) an identified or identifiable natural person and/or (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws), and (b) any information treated or receiving similar treatment as "personal data", "personal information", "personally identifiable information" or any similar, or equivalent terms under applicable Data Protection Laws;
- "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms "process", "processes" and "processed" will be interpreted accordingly;
- "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable the terms "processor", "service provider" and any equivalent or similar terms that address the same, or similar, responsibilities under applicable Data Protection Laws;
- "**Request**" means a request from a Data Subject or anyone acting on their behalf to exercise their rights under Data Protection Laws;
- "**Restricted Transfer**" means a transfer, or onward transfer, of Personal Data from a country where such transfer would be restricted or prohibited by applicable Data Protection Laws (or by the terms of a data transfer agreement put in place to address the data transfer restrictions of Data Protection Laws) without implementing safeguards such as the Standard Contractual Clauses to be established under clause 14 below;
- "**Security Documentation**" means the Documentation describing the security standards that apply to the Service as provided by or on behalf of Palantir from time to time;
- "**Sell**" or "**Sale**" 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.
- "**Service**" shall have the meaning as set out in the Agreement and this DPA.
- **"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, whether or not for monetary or other valuable consideration, including transactions in which no money is exchanged;
- "**Subprocessor**" means any processor or service provider who processes personal data on behalf of Palantir for the purpose of providing the Service as set out in the Agreement, Exhibit A and any other relevant applicable exhibits of this DPA.
- "**Standard Contractual Clauses**" or "**SCCs**" means either (a) the standard data protection clauses approved pursuant to the Data

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

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

2 TERM

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

3 SCOPE AND APPLICATION

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

4 ROLE OF THE PARTIES

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

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

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

5 CUSTOMER PROCESSING OF PERSONAL DATA

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

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

5.3 Customer shall have sole responsibility for the lawful Processing of Customer Personal Data in connection with its use of the Palantir Technology and/or its receipt of any related Professional Services in accordance with applicable Data Protection Laws, including without limitation, the accuracy, quality, and legality of the Customer Personal Data, the means by which it acquires and uses Customer Personal Data, and the Customer Instructions regarding the Processing of Customer Personal Data. Customer represents and warrants that it has (or its Controller has) a valid legal basis for the Processing of Customer Personal Data and has (or its Controller has) provided (or procured the provision of) all notifications and obtained (or procured the provision of) all consents (including Consents), 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.

6 PALANTIR PROCESSING OF CUSTOMER PERSONAL DATA

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

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

(b) not Sell or Share Customer Personal Data or otherwise retain, use, disclose, or Process Customer Personal Data outside of the direct business relationship between the Parties or for any purpose other than for the fulfilment of the Business Purposes

pursuant to Customer Instructions, unless obligated to do otherwise by applicable law or regulation or requests or orders of judicial, governmental or regulatory entities (including without limitation subpoenas), in which case Palantir will inform Customer of that legal requirement before such Processing occurs unless legally prohibited from doing so;

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

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

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

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

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

6.2 Customer shall instruct Palantir as to the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects taking into account the specific tasks and responsibilities of the Processor in the context of the Processing to be carried out and the risk to the rights and freedoms of the Data Subject as part of Customer Instructions. Notwithstanding anything to the contrary herein, Customer shall ensure that its acts or omissions, including in relation to any Customer Instructions to Palantir, do not put Palantir in breach of the Data Protection Laws.

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

7 SUBPROCESSORS

7.1 Customer specifically authorizes the engagement as Subprocessors of (a) the entities listed in Exhibit A and/or applicable specific additional Services exhibits in this DPA 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.

7.2 Subject to Section 7.3, 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.

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

8 AUDIT

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

8.2 At Customer's written request, Palantir will provide Customer with a confidential summary of the Report, documentation evidencing compliance with the Accreditations, and the Accountability Information outlined in Section 10 of this DPA so that Customer can reasonably verify Palantir's compliance with the data security and data protection obligations under this DPA. Subject to Section 8.3, if Data Protection Laws, Standard Contractual Clauses, or the Agreement 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.

8.3 In order to request an audit of Palantir's facilities under this Section 8 (and where such an audit is authorized), Customer shall notify Palantir 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 Customer shall bear the reasonable costs of Palantir in fulfilling any requirements under this Section. The scope of any audit under this Section 8 shall be limited to Palantir systems and facilities used to Process Customer Personal Data and Documentation directly related to such Processing.

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

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

9 DEALINGS WITH DATA PROTECTION AUTHORITIES AND DATA PROTECTION IMPACT ASSESSMENTS

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

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

10 ACCOUNTABILITY

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

(a) the name and contact details of the Processors and Subprocessors;

(b) details of the types of Processing being carried out;

(c) details of any transfers of Customer Personal Data to a territory or international organisation outside of the EEA or UK, and documentation of suitable safeguards (if applicable); and

(d) a general description of the technical and organisational security measures used in relation to the Processing,

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

11 DATA SUBJECT RIGHTS

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

11.2 The Service provides Customer with controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Personal Data. Customer may use these controls as technical and organisational measures to comply with its obligations under Data Protection Laws, to respond 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.

12 DATA INCIDENT

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

attacks; or any access to or Processing of Customer Personal Data that is consistent with Customer Instructions.

12.2 Palantir shall provide Customer with reasonable cooperation and assistance in dealing with a Data Incident, in particular in relation to (a) taking commercially reasonable steps to resolve any data privacy or security issues involving any Customer Personal Data; and (b) making any appropriate notifications to individuals affected by the Data Incident or to a Supervisory Authority to the extent reasonably possible; provided that, Customer shall maintain and follow an effective cyber incident response policy, which shall include the use of legal professional, litigation, or client attorney privilege, work in good faith with Palantir in relation to the Data Incident, and agree with Palantir the form and method of any public announcement in relation to the Data Incident.

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

13 DATA TRANSFERS

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

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

(a) The Parties shall hereby enter into a set of SCCs. The applicable SCCs and any required Completions as applicable and set out in Exhibit D, shall hereby be deemed incorporated into this DPA, and apply between Customer (as Exporter) and Palantir (as importer);

(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 any transfers of Customer Personal Data between Palantir and any Palantir third party Subprocessors, are subject to contractual terms between Palantir and the relevant third party Subprocessor providing appropriate safeguards and containing clauses equivalent to the SCCs.

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

14 LIABILITY

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

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

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

15 GOVERNING LAW AND JURISDICTION

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

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

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

16 GENERAL TERMS

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

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

EXHIBIT A

List of approved Subprocessors

Part I – Subprocessors

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

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

Authorized Third-Party Subprocessors				
Subprocessor	**Purpose**	**Registered Address**	**Location**	**Transfer Mechanism**
Amazon Web Services, Inc.	Cloud hosting and infrastructure, alerting and encrypted notification services and AI services.	410 Terry Avenue North, Seattle, WA 98109, USA	As selected by Customer in the Order Form or, as applicable, other parts of the Agreement.	Standard Contractual Clauses
Microsoft Corporation	Cloud hosting and infrastructure, and AI services (Microsoft Azure)	One Microsoft Way, Redmond, WA 98052, USA	The location for the purpose of providing the cloud hosting service is as selected by Customer in the Order Form or, as applicable, other parts of the Agreement. The location for the purpose of providing the AI services is East US, South Central US, West Europe and other Azure regions as they become available.	Standard Contractual Clauses
Google LLC	Cloud hosting and infrastructure (Google Cloud Platform) and AI services.	1600 Amphitheatre Parkway, Mountain View, 94043 CA, USA	The location for the purpose of providing the cloud hosting service is as selected by Customer in the Order Form or, as applicable, other parts of the Agreement. The location for the purpose of providing the AI services are all regions available for features of Generative AI on Google Vertex AI and other regions as they become available.	Standard Contractual Clauses

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 service can be the United States and other regions as they become available.	Standard Contractual Clauses

PART II – Palantir Affiliates

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

Exhibit A Updates

29 August 2023	Addition of alerting and encrypted notification services for the purpose of using AWS. This update is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
30 October 2023	Addition of OpenAI LLC as a Third-Party Subprocessor. Authorization for subprocessing by this additional subprocessor is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.
12 December 2023	General update to align this DPA with our global DPA terms, including edits to the Data Subject Rights and Data Transfers sections. This update is considered effective for Agreements entered on or after the date of this update, unless subject to separate written agreement between Palantir and Customer.

EXHIBIT B

Subject Matter and Details of Customer Personal Data Processing

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

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

Categories of Customer Personal Data

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

Subject Matter of Processing

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

Nature and Purpose of Processing

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

Duration of Processing

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

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

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

EXHIBIT C - APOLLO SERVICES

The following capitalized term will have the meaning indicated below:

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

EXHIBIT C-1

List of approved Subprocessors

PART I - Subprocessors

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

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

PART II - Palantir Affiliates

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

EXHIBIT C-2

Subject Matter and Details of Customer Personal Data Processing

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

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

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

Categories of Customer Personal Data

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

Subject Matter of Processing

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

Nature and Purpose of Processing

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

Duration of Processing

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

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

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

EXHIBIT D

Additions to the Standard Contractual Clauses

The following capitalized term will have the meaning indicated below:

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

"**Completions**" means

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iv) in relation to SCCs in relation to exports from Switzerland, the EU SCCs shall apply (incorporating the completions set out at (i)(a)-(g) above), as amended by 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 any other country, the completions set out in (i)(a)-(g) above shall be made or such other Completions as most closely achieves the same outcome as those Completions.

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

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

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

ANNEX 1 TO EXHIBIT D

STANDARD CONTRACTUAL CLAUSES

Module 2: Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) *(1)* for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix.

This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

[intentionally left blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data

subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union *(2)* (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 2 GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. *(3)* The Parties agree that, by

complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that

part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

[Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards *(4)*;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Name of Customer as stated in the Agreement.

Address: Address of Customer as stated in the Agreement.

Contact person's name, position and contact details: Point of contact for Customer as stated in the Agreement.

Activities relevant to the data transferred under these Clauses: Customer under the Agreement

Role (controller/processor): Controller

Data importer(s):

Name: Name of Palantir as stated in the Agreement.

Address: Address of Palantir as stated in the Agreement.

Contact person's name, position and contact details: Data Protection Officer, dpo@palantir.com

Activities relevant to the data transferred under these Clauses: Supplier under the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described under "Categories of Data Subject Whose Personal Data May be Subject to Processing" in Exhibit B and any other relevant exhibits for applicable additional Services.

Categories of personal data transferred

As described under "Categories of Customer Personal Data" in Exhibit B and any other relevant exhibits for applicable additional Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, data concerning a natural person's sex life or sexual orientation to the extent that Customer Personal Data includes such sensitive data and is provided to Palantir for Processing (including via the Service) by or at the direction of Customer or Customer's Users. In that case Customer shall clearly identify such sensitive data to Palantir in writing before providing such sensitive data. The applied safeguards and restrictions are described in Annex II.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

On a continuous basis.

Nature of the processing

As described under "Nature and Purpose of Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

Purpose(s) of the data transfer and further processing

As described under "Nature and Purpose of Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described under "Duration of Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described under "Subject matter, nature and duration of processing by sub-processors" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority as determined in accordance with Clause 13 and as further specified at https://edpb.europa.eu/about-edpb/about-edpb/members_en (as updated from time to time).

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

The security features and functionalities available to Customer described in clause 4.1 of the DPA, as further documented in the Security Documentation, and the technical and organisational measures described in clause (d) of the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The controls available to Customer described in clause 4.1 of the DPA, as further documented in the Security Documentation.

ANNEX 2 TO EXHIBIT D

STANDARD CONTRACTUAL CLAUSES

Module 3: Processor to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) *(5)* for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix.

This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

[Intentionally left blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ().

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the

appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union *(6)* (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 2 GENERAL WRITTEN AUTHORISATION: The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. *(7)* The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter

and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards *(8)*;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these

Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with

these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Name of Customer as stated in the Agreement.

Address: Address of Customer as stated in the Agreement.

Contact person's name, position and contact details: Point of contact for Customer as stated in the Agreement.

Activities relevant to the data transferred under these Clauses: Customer under the Agreement

Role (controller/processor): Processor

Data importer(s):

Name: Name of Palantir as stated in the Agreement.

Address: Address of Palantir as stated in the Agreement.

Contact person's name, position and contact details: Data Protection Officer, dpo@palantir.com

Activities relevant to the data transferred under these Clauses: Supplier under the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described under "Categories of Data Subject Whose Personal Data May be Subject to Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

Categories of personal data transferred

As described under "Categories of Customer Personal Data" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, data concerning a natural person's sex life or sexual orientation to the extent that Customer Personal Data includes such sensitive data and is provided to Palantir for Processing (including via the Service) by or at the direction of Customer or Customer's Users. In that case, Customer shall clearly identify such sensitive data to Palantir in writing before providing such sensitive data. The applied safeguards and restrictions are described in Annex II.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

On a continuous basis.

Nature of the processing

As described under "Nature and Purpose of Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

Purpose(s) of the data transfer and further processing

As described under "Nature and Purpose of Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described under "Duration of Processing" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described under "Subject matter, nature and duration of processing by sub-processors" in Exhibit B and, where applicable, any other relevant exhibits for applicable additional Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority as determined in accordance with Clause 13 and as further specified at https://edpb.europa.eu/about-edpb/about-edpb/members_en (as updated from time to time).

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

The security features and functionalities available to Customer described in clause 4.1 of the DPA, as further documented in the Security Documentation, and the technical and organisational measures described in clause 4.3(c) of the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

The controls available to Customer described in clause 4.1 of the DPA, as further documented in the Security Documentation.

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(3) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(4) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(5) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(7) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(8) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.