EEA DATA PROCESSING ADDENDUM

Version 2.0, 9.27.2021

This EEA Data Processing Addendum (this "*DPA*"), will, when signed by duly authorized representatives of both Parties, form a part of the Master Subscription Agreement (or other electronic agreement or mutually executed written agreement) (the "*Master Agreement*") and associated Order(s) between Datadog, Inc., a Delaware (USA) corporation ("*Datadog*") and _____ ("*Customer*") applicable to Customer's use of Services and reflects the Parties' agreement with regard to the Processing of EEA Personal Data. Capitalized terms not otherwise defined in this DPA will have the respective meanings assigned to them in the Master Agreement or Section 15 below. This DPA does not remove or lessen Customer's obligations with respect to Personal Data under the Master Agreement.

1. Scope. This DPA supplements the Master Agreement and unless indicated otherwise, applies exclusively to Datadog's provision of access to the Services under the Master Agreement and Order(s) agreed to between Customer and Datadog. If and to the extent Datadog Processes Customer Personal Data on behalf of a Participating Affiliate, Customer is entering into this DPA on behalf of itself and such Participating Affiliate to the extent required under applicable EU Data Protection Law. For purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include any relevant Participating Affiliate. Each Party will comply with all Applicable Laws with respect to its performance under this DPA, including the GDPR.

2. Roles.

2.1. Customer Personal Data. The Parties acknowledge and agree that Customer is the Controller and Datadog is the Processor with respect to the Processing of Customer Personal Data, and that this DPA and the Master Agreement constitute Customer's documented instructions regarding Datadog's Processing of Customer Personal Data. An overview of the categories of Data Subjects, types of Customer Personal Data being Processed and the nature and purpose of the Processing is provided in Annex 1 to Schedule B. Notwithstanding the foregoing, Datadog will inform Customer promptly if it becomes aware that Customer's instructions may violate applicable EU Data Protection Law.

2.2. Account Data. The Parties acknowledge and agree that Customer and Datadog are independent Controllers with respect to the Processing of Account Data, and each Party will comply with its obligations as a Controller and agrees to provide reasonable assistance as is necessary: (a) to each other to enable each Party to comply with any Data Subject access requests and to respond to any other queries or complaints from Data Subjects in accordance with the EU Data Protection Law; and (b) to each other to facilitate the handling of any Personal Data Breach as required under EU Data Protection Law.

3. Customer Responsibilities and Restrictions. Without limiting its responsibilities under the Master Agreement, Customer is solely responsible for ensuring that no special categories of Personal Data (GDPR Article 9) or Personal Data relating to criminal convictions and offenses (GDPR Article 10) are submitted for Processing by the Services. Further, no provision of this DPA includes the right to, and Customer shall not, directly or indirectly, enable any person or entity other than Authorized Users to access and use the Services or use (or permit others to use) the Services other than as described in the applicable Order, Documentation, AUP, Master Agreement and this DPA, or for any unlawful purpose.

4. Duration. Unless earlier terminated as provided herein, the term of this DPA will continue through the expiration or earlier termination of the last applicable Order to be in effect.

5. Security. 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 Data Subjects, Datadog shall implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk (including those outlined in Annex II of Schedule A for Account Data, and those outlined in Annex II or Schedule B for Customer Personal Data (together, "*Security Measures*"). In assessing the appropriate level of security, Datadog shall take into account the risks that are presented by Processing Customer Personal Data including, in particular, the risks presented by a Customer Personal Data Breach (as defined in Section 9). Datadog may make such changes to the Security Measures as Datadog deems necessary or appropriate from time to time, including without limitation to comply with Applicable Law, but no such changes will reduce the overall level of protection for Customer Personal Data. Datadog will

take appropriate steps to ensure compliance with the Security Measures by its employees, agents, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to Process Customer Personal Data have agreed to appropriate obligations of confidentiality.

6. Subprocessors.

6.1. Customer authorizes Datadog's use of Datadog's Affiliates as Subprocessors and both Datadog's and its Affiliates' use of third-party Subprocessors in connection with the provision of Services. As a condition to permitting a Subprocessor to Process Customer Personal Data, Datadog or a Datadog Affiliate will enter into a written agreement with the Subprocessor containing data protection obligations no less protective than those in this DPA with respect to Customer Personal Data. Datadog will restrict its Subprocessors' access to only what is necessary to maintain the Services or to provide the Services to Customer and Authorized Users. Subject to this Section 6, Datadog reserves the right to engage and substitute Subprocessors as it deems appropriate, but shall: (a) remain responsible to Customer for the provision of the Services and (b) be liable for the actions and omissions of its Subprocessors undertaken in connection with Datadog's performance of this DPA to the same extent Datadog would be liable if performing the Services directly.

6.2. Datadog's current Subprocessors are listed in the Subprocessor List. Upon execution of this DPA, Datadog will subscribe Customer's email address listed on the signature page of this DPA to notifications of Datadog's use of new Subprocessors ("*Change Notices*"). Datadog will send a Change Notice before a new Subprocessor Processes any Customer Personal Data. Customer may object to any new Subprocessor on reasonable grounds relating to the protection of the Customer Personal Data, in which case Datadog shall have the right to satisfy the objection through one of the following:

(a) Datadog will cancel its plans to use the Subprocessor with regard to Customer Personal Data or will offer an alternative to provide the Services without such Subprocessor;

(b) Datadog will take the corrective steps requested by Customer in its Objection Notice (which remove Customer's objection) and proceed to use the Subprocessor with regard to Customer Personal Data; or

(c) Datadog may cease to provide, or Customer may agree not to use (temporarily or permanently), the particular aspect of the Services that would involve the use of such Subprocessor with regard to Personal Data, subject to a mutual agreement of the Parties to adjust the remuneration for the Services considering their reduced scope.

6.3. All objections under Section 6.2 must be submitted by email to Datadog at privacy@datadoghq.com within 14 days of the Change Notice (each, an "*Objection Notice*"). If none of the options outlined in Clause (a), (b) or (c) of Section 6.2 are reasonably available and Customer's objection has not been resolved to the Parties' mutual satisfaction within 30 days of Datadog's receipt of the Objection Notice, either Party may terminate the affected Order and Datadog will refund to Customer a pro rata share of any unused amounts prepaid by Customer under the applicable Order for the Services on the basis of the remaining portion of the current terms of the Order.

6.4. If the Customer does not provide a timely Objection Notice with respect to a new Subprocessor, Customer will be deemed to have authorized Datadog to use of the Subprocessor and to have waived its right to object. Datadog may use a new or replacement Subprocessor while the objection procedures under this Section 6 are in process.

7. Data Subject Rights. If Datadog receives a request from a Data Subject in relation to Customer Personal Data then, to the extent legally permissible, Datadog will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services. Customer hereby agrees that Datadog may confirm to a Data Subject that his or her requests relates to Customer. To the extent Customer is unable through its use of the Services to address a particular Data Subject request, Datadog will, upon Customer's request and taking into account the nature of Customer Personal Data Processed, provide reasonable assistance in addressing the Data Subject request (provided Datadog is legally permitted to do so and that the Data Subject request was made in accordance with EU Data Protection Law). To the extent permitted by Applicable Law, Customer shall be responsible for any costs arising from Datadog's provision of such assistance.

8. Deletion Upon Expiration. Commencing 30 days after the effective date of termination of the Master Agreement, Datadog will initiate a process upon Customer's written request that deletes Customer Personal Data retained in production within 90 days and in backups within 180 days. Any Customer Personal Data archived in backups will be isolated and protected from any further Processing, except as otherwise required by Applicable Law. Notwithstanding the foregoing, to

the extent Datadog is required by Applicable Law to retain some or all Customer Personal Data, Datadog will not be obligated to delete the retained Customer Personal Data, but this DPA will continue to apply to the retained Customer Personal Data. Customer acknowledges that it is responsible for exporting any Customer Data that Customer wants to retain prior to expiration of the referenced 30-day period pursuant to the Master Agreement.

9. Customer Personal Data Breach Management. Datadog will notify Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach with respect to Customer Personal Data transmitted, stored or otherwise Processed by Datadog or its Subprocessors (a "*Customer Personal Data Breach*"). Such notice may be provided (1) by posting a notice in the Services; (2) by sending an email to the email address from which a Change Notice subscription request was made; (3) by sending an email to the email address for Customer listed on the signature page to this DPA; and/or (4) pursuant to the notice provisions of the Master Agreement. Customer shall ensure that its contact information is current and accurate at all times during the terms of this DPA. Datadog will promptly take all actions relating to its Security Measures (and those of its Subprocessors) that it deems necessary and advisable to identify and remediate the cause of a Customer Personal Data Breach. In addition, Datadog will promptly provide Customer with: (i) reasonable cooperation and assistance with regard to the Customer Personal Data Breach, (ii) reasonable information in Datadog's possession concerning the Customer Personal Data Breach insofar as it affects Customer, including remediation efforts and any notification to Supervisory Authorities and, (iii) to the extent known: (a) the possible cause of the Customer Personal Data Breach; (b) the categories of Customer Personal Data involved; and (c) the possible consequences to Data Subjects. Datadog's notification of or response to a Customer Personal Data Breach under this Section will not constitute an acknowledgment of fault or liability with respect to the Customer Personal Data Breach, and the obligations herein shall not apply to Personal Data Breaches that are caused by Customer, Authorized Users or providers of Customer Components. If Customer decides to notify a Supervisory Authority, Data Subjects or the public of a Customer Personal Data Breach, Customer will provide Datadog with advance copies of the proposed notices and, subject to Applicable Law (including any mandated deadlines under EU Data Protection Law), allow Datadog an opportunity to provide any clarifications or corrections to those notices. Subject to Applicable Law, Datadog will not reference Customer in any public filings, notices or press releases associated with the Customer Personal Data Breach without Customer's prior consent.

10. Compliance and Reviews.

10.1. As of the date of this DPA, Datadog participates in the Cloud Security Alliance STAR self-assessment program and has completed the associated Consensus Assessments Initiative Questionnaire (CAIQ), currently available at https://cloudsecurityalliance.org/star/registry/datadog/. Subject to the confidentiality obligations of the Master Agreement, Datadog will additionally make available to Customer upon request such other attestations, certifications, reports or extracts thereof from external auditors or organizations as Datadog may possess from time to time to assist Customer in assessing Datadog's compliance with the terms of this DPA.

10.2. Where required by EU Data Protection Law, Datadog will allow Customer (directly or through a third-party auditor subject to written confidentiality obligations) to conduct an audit of Datadog's procedures relevant to the protection of Customer Personal Data to verify Datadog's compliance with its obligations under this DPA. In such case:

(a) Customer shall: (i) provide Datadog at least 30 days' prior written notice of any proposed audit; (ii) undertake an audit no more than once in any 12-month period, except where required by a competent Supervisory Authority or where an audit is required due to a Customer Personal Data Breach; and (iii) conduct any audit in a manner designed to minimize disruption of Datadog's normal business operations. To that end and before the commencement of any such audit, Customer and Datadog shall mutually agree upon the audit's participants, schedule and scope, which shall in no event permit Customer or its third-party auditor to access the Services' hosting sites, underlying systems or infrastructure.

(b) Customer shall reimburse Datadog for its time expended in connection with an audit at Datadog's then-current professional service rates, which shall be made available to Customer upon request and shall be reasonable taking into account the time and effort required by Datadog.

(c) Representatives of Customer performing an audit shall protect the confidentiality of all information obtained through such audits in accordance with the Master Agreement, may be required to execute an enhanced mutually agreeable nondisclosure agreement and shall abide by Datadog's security policies while on Datadog's premises. Upon completion of an audit, Customer agrees to promptly furnish to Datadog any written audit report or, if no

written report is prepared, to promptly notify Datadog of any non-compliance discovered during the course of the audit.

11. Impact Assessment and Additional Information. Datadog will provide Customer with reasonable cooperation, information and assistance as needed to fulfill Customer's obligation under EU Data Protection Law, including as needed to carry out a data protection impact assessment related to Customer's use of the Services (in each case to the extent Customer does not otherwise have access to the relevant information, and such information is in Datadog's control). Without limiting the foregoing, Datadog shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section to the extent required by EU Data Protection Law.

12. Transfer Mechanisms. The Standard Contractual Clauses – Controller to Controller (Schedule A) and the Standard Contractual Clauses – Controller to Processor (Schedule B) will apply, respectively, to Account Data and Customer Personal Data when transferred outside of the EEA to any country not recognized by the European Commission as providing an adequate level of data protection. Subject to Applicable Law, the Parties agree that the audits described in Clause 8.9 of Schedule B shall be carried out as set forth in Section 10 above, and that Datadog's use of subprocessors under Clause 9 of Schedule B shall be carried out as set forth in Section 6 above.

13. Limitation of Liability. Each Party's (and each of its Affiliate's) liability taken together in the aggregate, arising out of or related to this DPA, including without limitation under the Standard Contractual Clauses, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the Master Agreement.

14. Definitions.

14.1. Terms such as "*Personal Data*", "*Data Subject*", "*Processing*", "*Controller*", "*Processor*", "*Personal Data Breach*", and "*Supervisory Authority*" that are defined in Article 4 of the General Data Protection Regulation 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 of Directive 95/46/EC ("*GDPR*") shall have the meanings assigned to them in such Article.

14.2. Other capitalized terms not otherwise defined in this DPA shall have the respective meanings assigned to them in this Section.

"*Account Data*" means information about Customer that Customer provides to Datadog in connection with the creation or administration of its Datadog accounts, such as first and last name, user name and email address of an Authorized User or Customer's billing contact. Customer shall ensure that all Account Data is current and accurate at all times during the term of the applicable Order.

"*Adequacy*" means where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question, ensures an adequate level of protection.

"*Affiliate*" means, unless otherwise defined in the Master Agreement, a business entity that directly or indirectly controls, is controlled by or is under common control with, such Party; "control" means the direct or indirect ownership of more than 50% of the voting securities of a business entity.

"*Applicable Laws*" means any and all governmental laws, rules, directives, regulations or orders that are applicable to a particular Party's performance under this DPA, including applicable EU Data Protection Law.

"*AUP*" means Datadog's standard Acceptable Use Policy, currently available at https://www.datadoghq.com/legal/acceptable-use/.

"*Authorized User*" means an individual employee, agent or contractor of Customer or a Participating Affiliate for whom subscriptions to Services have been purchased pursuant to the terms of the Master Agreement and applicable Order, and who have been supplied user credentials for the Services by Customer or the Participating Affiliate (or by Datadog at Customer's or a Participating Affiliate's request).

"*Customer Component*" means each individual component of Customer's Environment.

"*Customer Credentials*" means access passwords, keys, tokens or other credentials used by Customer in connection with the Services.

"*Customer Data*" means data from Customer's Environment that are submitted for Processing by the Services. Through Customer's configuration and use of the Services, Customer has control over the types and amounts of Customer Data.

"*Customer's Environment*" means, exclusive of Services, the systems, platforms, services, software, devices, sites and/or networks that Customer uses in its own internal business operations.

"*Customer Personal Data*" means Customer Data comprising Personal Data of Data Subjects located in the EEA.

"*Documentation*" means Datadog's standard user documentation for the Services, currently available at https://docs.datadoghq.com/.

"*EEA*" means the European Economic Area, which constitutes the member states of the European Union ("*EU*") and Norway, Iceland and Liechtenstein, as well as for purposes of this DPA, the United Kingdom.

"*EU Data Protection Law*" means the GDPR, and shall include the data protection or privacy laws of the United Kingdom in place after its withdrawal from the EU.

"*Order*" means a separate order for Services pursuant to the Master Agreement: (a) completed and submitted by Customer online at the Datadog site and accepted by Datadog or (b) executed by Datadog and Customer.

"*Participating Affiliate*" means an Affiliate of Customer that: (a) has not entered into an Order or other separate agreement directly with Datadog and (b) Customer has authorized to access and use the Services under an existing Order between Datadog and Customer.

"*Party*" means each of Datadog and Customer.

"*Services*" means the hosted services to which Customer subscribes through, or otherwise uses following, an Order that are made available by Datadog online via the applicable login page (currently https://app.datadoghq.com/) and other web pages designated by Datadog. Subject to the terms of an Order, the Services will support Customer's collection, monitoring, management and analysis of Customer Data. For purposes of this DPA, the term Services does not include alpha, beta or other pre-commercial releases of a Datadog product or service (or feature of functionality of a Service).

"*Standard Contractual Clauses*" means the agreements executed by and between Datadog and Customer and attached to this DPA as Schedule A and Schedule B pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"*Subprocessor*" means any Processor engaged by Datadog or a Datadog Affiliate to Process Customer Personal Data on Datadog's or its Affiliate's behalf in the course of providing the Services.

"*Subprocessor List*" means the list of Subprocessors available at https://www.datadoghq.com/subprocessors/.

15. Counterparts. This DPA, including the attached Standard Contractual Clauses, may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. Delivery of an executed counterpart of a signature page to this DPA by fax or by email of a scanned copy, or execution and delivery through an electronic signature service (such as DocuSign), shall be effective as delivery of an original executed counterpart of this DPA.

IN WITNESS WHEREOF, the Parties hereto have executed this DPA as of the Effective Date.

DATADOG, INC.	**CUSTOMER**
By:_____ Name: Title: Date:	By:_____ Name: Title: Date:
	Customer address (required): Customer email (required):

SCHEDULE A - CONTROLLER TO CONTROLLER STANDARD CONTRACTUAL CLAUSES

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) 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority

pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors - *Omitted*

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or 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;

(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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: The entity identified as "Customer" in the DPA.

Address: Customer's address identified in the DPA.

Contact person's name, position and contact details:

Name: _____

Position: _____

Email: _____

Phone Number: _____

Activities relevant to the data transferred under these Clauses: The Processing of Account Data for the purpose of providing the Services to which exporter has subscribed.

Signature and date:

Name: _____

Signature: _____

Date: _____

Role (controller/processor): Controller.

Data importer(s):

1. Name: Datadog, Inc.

Address: 620 8th Ave., 45th Fl., New York, NY 10018 USA

Contact person's name, position and contact details: Darlene Cedres, Head of Privacy and Associate General Counsel; darlene.cedres@datadoghq.com.

Activities relevant to the data transferred under these Clauses: The Processing of Account Data for the purpose of providing the Services to which exporter has subscribed.

Signature and date:

Name: _____

Signature: _____

Date: _____

Role (controller/processor): Controller.

B. DESCRIPTION *OF TRANSFER*

Categories of data subjects whose personal data is transferred

Exporter's Authorized Users.

Categories of personal data transferred

The personal data in Account Data that is sent to importer by exporter for the purpose of using the 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.

No sensitive data is transferred.

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

The personal data is transferred on a continuous basis.

Nature of the processing

General account management and other activities as outlined in Datadog's public Privacy Policy, available at https://www.datadoghq.com/legal/privacy/.

Purpose(s) of the data transfer and further processing

For importer to (a) manage exporter's account, including to calculate Fees; (b) provide and improve the Services and Support, including to address Support Requests and troubleshoot other issues; and (c) provide exporter and Authorized Users with insights, service and feature announcements, and other reporting.

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

Personal data is retained to manage exporter's accounts in accordance with Datadog's Privacy Policy.

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

The subject matter of personal data transferred to subprocessors is Account Data, which is transferred to subprocessors in order to manage exporter's accounts with importer, in accordance with Datadog's Privacy Policy.

C. COMPETENT *SUPERVISORY AUTHORITY*

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

[TO BE ADDED]

ANNEX II

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

As of the date of this DPA, the data importer's technical and organisational include the following.

1. **Access Control**
   - Datadog restricts access to Customer Personal Data to employees with a defined need-to-know or a role requiring such access.
   - Datadog maintains user access controls that address timely provisioning and de-provisioning of user accounts.

2. **Audit**
   - Datadog will maintain SSAE 18 SOC 2 certification, or comparable certification, for the term of the Master Agreement. This certification will be renewed on an annual basis. Upon Customer's request, Datadog will provide a summary of its most recent SOC 2 report once every 12 months of the term of the Master Agreement.
   - Datadog follows guidelines from ISO 27001, NIST and other industry-standard practices.

3. **Business Continuity**
   - Datadog maintains business continuity, backup and disaster recovery plans ("BC/DR Plans") in order to minimize the loss of service and comply with Applicable Laws.
   - The BC/DR Plans address threats to the Services and any dependencies, and have an established procedure for resuming access to, and use of, the Services.
   - The BC/DR Plans are tested at regular intervals.

4. **Change Control**
   - Datadog maintains policies and procedures for applying changes to the Services, including underlying infrastructure and system components, to ensure quality standards are being met.
   - Datadog undergoes a penetration test of its network and Services on an annual basis. Any vulnerabilities found during this testing will be remediated in accordance with Datadog's Vulnerability Management Policies and Procedures, and will be assessed on the basis of Datadog's Risk Management Framework.
   - Datadog performs monthly scans of its network and any vulnerabilities found will be addressed in accordance with Datadog's Vulnerability Management Policies and Procedures, and will be assessed on the basis of Datadog's Risk Management Framework.
   - Security patches are applied in accordance with Datadog's patching schedule.

5. **Data Security**
   - Datadog maintains technical safeguards and other security measures to ensure the security and confidentiality of Customer Personal Data.
   - Datadog logically segregates Customer Data in the production environment.

6. **Encryption and Key Management**
   - Datadog maintains policies and procedures for the management of encryption mechanisms and cryptographic keys in Datadog's cryptosystem.
   - Datadog enlists encryption at rest and in transit between public networks, as applicable, according to industry-standard practice.

7. **Governance and Risk Management**
   - Datadog maintains an information security program that is reviewed at least annually.
   - Datadog maintains a risk management program, with risk assessments conducted at least annually.

8. **Infrastructure Security**
   - Datadog maintains system clock synchronization across all applicable systems in relation to the Services.
   - Datadog maintains an environment for testing and development separate from the production environment.

SCHEDULE B – CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

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) 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 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 Union4 (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 benefiting 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) 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 subprocessors at least thirty (30) 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. 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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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;

(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

[OPTION 1: 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.

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ *(specify Member State)*.]

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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: The entity identified as "Customer" in the DPA.

Address: Customer's address identified in the DPA.

Contact person's name, position and contact details:

Name: _____

Position: _____

Email: _____

Phone Number: _____

Activities relevant to the data transferred under these Clauses: Providing, supporting, and improving the Services to which exporter has subscribed.

Signature and date:

Name: _____

Signature: _____

Date: _____

Role (controller/processor): Controller.

Data importer(s):

1. Name: Datadog, Inc.

Address: 620 8th Ave., 45th Fl., New York, NY 10018 USA

Contact person's name, position and contact details: Darlene Cedres, Head of Privacy and Associate General Counsel; darlene.cedres@datadoghq.com.

Activities relevant to the data transferred under these Clauses: Importer will process Customer Personal Data to (a) provide the Services in accordance with the features and functionality of the Services and the Documentation; (b) enable Authorized User-initiated actions on and through the Services; (c) as set forth in the Master Agreement and applicable Order(s); and (d) as further documented by written instructions given by Customer Providing, supporting, and improving the Services to which exporter has subscribed.

Signature and date:

Name: _____

Signature: _____

Date: _____

Role (controller/processor): Processor.

B. DESCRIPTION *OF TRANSFER*

Categories of data subjects whose personal data is transferred

Exporter's Authorized Users, customers, vendors, and end users.

Categories of personal data transferred

The personal data in Customer Data that is sent to importer by exporter for the purpose of using the 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.

No sensitive data is transferred.

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

The personal data is transferred on a continuous basis.

Nature of the processing

Analysis, storage, and other Services as described in the Master Agreement, Order(s), DPA, and Documentation.

Purpose(s) of the data transfer and further processing

For importer to provide, support, and improve the Services.

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

Personal data is retained in accordance with either exporter's configuration of the Services or the retention schedules outlined in the Documentation.

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

The subject matter of personal data transferred to subprocessors is Customer Data, which is transferred to subprocessors in order to provide, support, and improve the Services, as outlined in the agreements between the exporter and the importer.

C. COMPETENT *SUPERVISORY AUTHORITY*

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

[TO BE ADDED]

ANNEX II

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

As of the date of this DPA, the data importer's technical and organisational include the following.

1. **Access Control**
   - Datadog restricts access to Customer Personal Data to employees with a defined need-to-know or a role requiring such access.
   - Datadog maintains user access controls that address timely provisioning and de-provisioning of user accounts.

2. **Audit**
   - Datadog will maintain SSAE 18 SOC 2 certification, or comparable certification, for the term of the Master Agreement. This certification will be renewed on an annual basis. Upon Customer's request, Datadog will provide a summary of its most recent SOC 2 report once every 12 months of the term of the Master Agreement.
   - Datadog follows guidelines from ISO 27001, NIST and other industry-standard practices.

3. **Business Continuity**
   - Datadog maintains business continuity, backup and disaster recovery plans ("BC/DR Plans") in order to minimize the loss of service and comply with Applicable Laws.
   - The BC/DR Plans address threats to the Services and any dependencies, and have an established procedure for resuming access to, and use of, the Services.
   - The BC/DR Plans are tested at regular intervals.

4. **Change Control**
   - Datadog maintains policies and procedures for applying changes to the Services, including underlying infrastructure and system components, to ensure quality standards are being met.
   - Datadog undergoes a penetration test of its network and Services on an annual basis. Any vulnerabilities found during this testing will be remediated in accordance with Datadog's Vulnerability Management Policies and Procedures, and will be assessed on the basis of Datadog's Risk Management Framework.
   - Datadog performs monthly scans of its network and any vulnerabilities found will be addressed in accordance with Datadog's Vulnerability Management Policies and Procedures, and will be assessed on the basis of Datadog's Risk Management Framework.
   - Security patches are applied in accordance with Datadog's patching schedule.

5. **Data Security**
   - Datadog maintains technical safeguards and other security measures to ensure the security and confidentiality of Customer Personal Data.
   - Datadog logically segregates Customer Data in the production environment.

6. **Encryption and Key Management**
   - Datadog maintains policies and procedures for the management of encryption mechanisms and cryptographic keys in Datadog's cryptosystem.
   - Datadog enlists encryption at rest and in transit between public networks, as applicable, according to industry-standard practice.

7. **Governance and Risk Management**
   - Datadog maintains an information security program that is reviewed at least annually.
   - Datadog maintains a risk management program, with risk assessments conducted at least annually.

8. **Infrastructure Security**
   - Datadog maintains system clock synchronization across all applicable systems in relation to the Services.

DATADOG MAINTAINS AN ENVIRONMENT FOR TESTING AND DEVELOPMENT SEPARATE FROM THE PRODUCTION ENVIRONMENT.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Service Providers

Name	Address	Description of processing
Amazon Web Services, Inc.	410 Terry Avenue North Seattle, WA 98109 United States	Datadog customers can deploy solutions on an AWS cloud computing environment that provides compute, power, storage, and other application services over the Internet as their business needs demand.
Atlassian Pty Ltd (Jira)	350 Bush Street, Floor 13 San Francisco, CA 94104 United States	Datadog uses Jira issue-tracking software to manage support requests from customers.
Google LLC (G Suite)	1600 Amphitheatre Pkwy Mountain View, CA 94043 United States	Datadog uses this office suite to (1) communicate with customers in some cases, and (2) manage and organize customer requests.
Google LLC (Google Cloud Platform)	1600 Amphitheatre Pkwy Mountain View, CA 94043 United States	Datadog customers can deploy solutions on a GCP cloud-computing environment that provides compute, power, storage, and other application services over the Internet as their business needs demand.
Mailgun Technologies, Inc.	112 E Pecan St #1135 San Antonio, TX 78205 United States	Datadog uses this (1) as a backup email relay to send emails to Datadog customers or customer's users as part of the Datadog services (including, for example, monitor alerts, reports, and account modification), and (2) to receive emails from services or people (e.g., emails from help@datadoghq.com).
Microsoft Corporation (Azure)	Attn: Chief Privacy Officer 1 Microsoft Way Redmond, WA 98052 United States	Datadog customers can deploy solutions on a Microsoft Azure cloud computing environment that provides compute, power, storage, and other application services over the Internet as their business needs demand.
SendGrid, Inc.	375 Beale St #300 San Francisco, CA 94105 United States	Datadog uses this (1) as a primary email relay to send emails to Datadog customers or customer's users as part of the Datadog services (including, for example, monitor alerts, reports, and account modification), and (2) to receive emails from services or people (e.g., emails from help@datadoghq.com).
Slack Technologies, Inc.	500 Howard Street San Francisco, CA, 94105 United States	Datadog uses this internal-collaboration tool and communication platform to manage support requests from customers.
Snowflake, Inc.	106 East Babcock Street Suite 3A Bozeman, MT 59715 United States	Datadog uses Snowflake to securely house data for analytics purposes.
Trello, Inc.	350 Bush Street, Floor 13 San Francisco, CA 94104 United States	Datadog uses this issue-tracking software to manage support requests from customers.
Zendesk, Inc.	989 Market Street San Francisco, CA 94103 United States	Datadog uses this customer-service software to manage and resolve support requests from customers.

Affiliates

Name	Address	Description of processing

Datadog France SAS	21 Rue de Châteaudun 6th Floor 75009 Paris France	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Germany GmbH	Hermannstraße 13 c/o WeWork 20095 Hamburg Germany	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Ireland Limited	70 Sir John Rogersons Quay Dublin 2 Ireland	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Japan G.K.	Tokyo Club Building 11F 3-2-6 Kasumigaseki Chiyoda-ku Tokyo 100-0013 Japan	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Korea, Inc.	Daechi-dong #115, 19F Seolleung-ro, 428 Gangnam-gu Seoul South Korea	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Netherlands BV	Prins Bernhardplein 200 1097 JB Amsterdam Netherlands	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Services Canada, Inc.	c/o McCarthy Tétrault LLP Suite 2400 745 Thurlow Street Vancouver, BC V6E 0C5 Canada	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.
Datadog Singapore Pte. Ltd.	c/o TMF Singapore Pte. Ltd. 38 Beach Road #29-11 South Beach Tower Singapore 189767	This Datadog affiliate employs individuals for the purpose of technical customer and sales support.