DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the terms of service, master service agreement or other agreement that govern the purchase of Services ("**Service Agreement**") between **Treasure Data, Inc.** and the counterparty therein ("**Customer**") by referencing this DPA. This DPA governs the Parties' responsibilities with regard to the Processing of Personal Data by Treasure Data for Customer in connection with the provision of the Service. Customer and Treasure Data are hereunder jointly referred to as the "**Parties**", and each separately as a "**Party**".

1. DEFINITIONS

For the purposes of this DPA, the following capitalized words are ascribed the following meanings. All capitalized terms not defined in this DPA shall have the meaning ascribed to them in the Service Agreement.

1.1 "**Agreement**" means the Service Agreement together with this DPA.

1.2 "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.3 "**Collected Data**" means any data and information submitted by or for Customer to the Service as defined in the Service Agreement.

1.4 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.5 **"Data Subject Request"** has the meaning ascribed to it under Clause 4.2.

1.6 "**Data Protection Legislation**" means all laws and regulations relating to the protection of personal data and privacy of individuals (amended, superseded or replaced from time to time), including without limitation the California Consumer Privacy Act, the GDPR, the European Directive 2002/58/EC (as amended by Directive 2009/136/EC), Personal Information Protection and Electronic Documents Act, and Act on the Protection of Personal Information of Japan (Act No. 57 of 2003, as amended, the "Japanese Act", of which English translation is available at https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

1.7 "**Documented Instructions**" has the meaning ascribed to it under Clause 3.2.

1.8 "**DPA**" has the meaning ascribed to it above.

1.9 **"EEA"** means the European Economic Area.

1.10 **"European Data Protection Legislation"** means, as applicable, the GDPR, the UK GDPR and the Federal Data Protection Act of 19 June 1992 (Switzerland), each as amended, superseded or replaced from time to time.

1.11 "**GDPR**" means the 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), as amended, superseded or replaced from time to time.

1.12 "**Personal Data**" means any information relating to an identified or identifiable natural person included in Collected Data.

1.13 "**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Treasure Data under the Agreement.

1.14 "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.15 "**Service"** means the services provided by Treasure Data under the Service Agreement.

1.16 **"Service Agreement"** has the meaning ascribed to it above.

1.17 "**Processor**" means the entity which Processes Personal Data on behalf of a Controller.

1.18 "**Relevant Transfer**" has the meaning ascribed to it under Clause 7.3.

1.19 "**Standard Contractual Clauses**" means clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, attached hereto as Schedule 1.

1.20 "**Sub-processor**" means a third party that Treasure Data engages for the Processing of Personal Data on behalf of Customer.

1.21 "**Supervisory Authority**" means an independent public authority charged with overseeing the compliance with Data Protection Legislation.

1.22 **"UK"** means the United Kingdom.

1.23 **"UK GDPR"** means the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, as amended, superseded or replaced from time to time.

2. ROLES OF THE PARTIES

2.1 Customer shall, in its use of the Service, Process Personal Data at all times in accordance with the requirements of the applicable Data Protection Legislation and any other laws and regulations applicable to Customer and in accordance with the Agreement.

2.2 As between Customer and Treasure Data, Customer has sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Personal Data were acquired.

2.3 If Customer is not the Controller of the Personal Data, or is a Controller jointly with others, Customer represents and warrants to Treasure Data that any third party who is a Controller of the Personal Data agrees to the Processing by Treasure Data of the Personal Data pursuant to the Agreement and the Documented Instructions provided to Treasure Data pursuant to the Agreement.

2.4 Customer acts as a single point of contact and is responsible for obtaining any relevant authorizations, consents and permissions for the Processing of Personal Data in accordance with the Agreement. Where authorizations, consent, instructions or permissions are provided by Customer, these are provided not only on behalf of Customer but also on behalf of all relevant Controllers of the Personal Data. Where Treasure Data informs or gives notice to Customer, it is Customer's responsibility to forward such information and notices to any relevant Controller(s) (as applicable) without undue delay.

3. CUSTOMER'S INSTRUCTIONS AND CONFIDENTIALITY

3.1 The subject matter of Processing of Personal Data by Treasure Data in the performance of the Service pursuant to the Service Agreement, the duration, the nature and purpose of such Processing, the types of Personal Data Processed under the Service Agreement and relevant categories of Data Subjects are specified in Schedule 2 to this DPA.

3.2 The Parties agree that this DPA and the Service Agreement and the instructions provided via configuration or other tools made available by Treasure Data under the Service Agreement (such as APIs or SDKs) constitute Customer's documented instructions regarding Treasure Data's Processing of Personal Data under the Agreement ("**Documented Instructions**"). The Documented Instructions shall comply with applicable Data Protection Legislation and any other laws and regulations applicable to Customer.

3.3 If, in Treasure Data's opinion, any Documented Instruction infringes Data Protection Legislation, Treasure Data will immediately inform Customer. For the avoidance of doubt, this Clause 3.3 does not imply an obligation on Treasure Data to conduct any legal review of any Documented Instruction and any communication or information provided by Treasure Data to Customer pursuant to this Clause 3.3 is not and shall not be deemed to be legal advice.

3.4 Treasure Data shall process Personal Data in accordance with the Documented Instructions, unless otherwise required by law to which Treasure Data is subject. In such a case, Treasure Data shall inform Customer of such legal requirement before Processing, unless the law prohibits such disclosure.

3.5 Any instruction related to the Processing of Personal Data additional to the Documented Instructions require prior written agreement between the Parties, including agreement on any additional fees payable by Customer to Treasure Data for carrying out such instruction. Once agreed, any such additional instruction is deemed as a Documented Instruction under this DPA.

3.6 Where Standard Contractual Clauses apply between the Parties, the Documented Instructions are deemed to be the instructions by the Customer for the purpose of Clause 5(a) of the Standard Contractual Clauses.

3.7 Treasure Data shall not disclose Personal Data to any third party except as permitted under the Agreement or as necessary to comply with the law or a valid and binding order of a governmental body. If Treasure Data is required to disclose Personal Data to a governmental body, then Treasure Data will use commercially reasonable efforts to give Customer notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Treasure Data is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Clause 3.7 varies or modifies the Standard Contractual Clauses.

3.8 Treasure Data shall ensure that persons it authorizes to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. OBLIGATIONS TO ASSIST

4.1 Treasure Data shall, taking into account the information available to Treasure Data and the nature of the Processing, provide reasonable assistance to Customer as required under applicable Data Protection Legislation in ensuring compliance with Customer's obligations relating to data protection impact assessments and prior consulting obligations with the competent Supervisory Authority. Treasure Data may charge Customer for reasonable costs and expenses incurred as a result of such assistance.

4.2 Treasure Data shall, to the extent legally permitted, promptly notify Customer if Treasure Data receives a request from a Data Subject to exercise the Data Subject's right granted under the applicable Data Protection Legislation ("**Data Subject Request**"). To the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Treasure Data shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Treasure Data is legally permitted to do so.

5. DATA SECURITY AND DATA BREACHES

5.1 Treasure Data has implemented and will maintain appropriate technical and organizational measures ("**Security Measures**") intended to protect Personal Data Processed under the Agreement against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. Treasure Data's Security Measures applicable to the Service provided under the Service Agreement are further described at Schedule 3 to this DPA.

5.2 Customer agrees that Treasure Data may modify at any time at its discretion the Security Measures, provided that Treasure Data does not decrease the overall security of the Service during the term of the Agreement and continues to comply with Clause 5.1 above. From time to time the most up to date description of the Security Measures will be made available on Treasure Data's website (www.treasuredata.com/terms/) or communicated to Customer in writing.

5.3 In the event of a Personal Data Breach, Treasure Data shall notify Customer promptly without undue delay after becoming aware of the Personal Data Breach. The notification shall contain information that Treasure Data is reasonably able to disclose to Customer, including the following information (which may be provided in phases if it is not possible to provide the information at the same time): (a) a description of the nature of the Personal Data Breach including, the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned; (b) the name and contact details of contact point where more information can be obtained; (c) a description of the likely consequences of the Personal Data Breach; and (d) a description of the measures taken or proposed to be taken to address the Personal Data Breach. Customer shall provide notice of the Personal Data Breach to the Data Subjects and Supervisory Authority as it determines necessary, and Treasure Data shall provide reasonable cooperation and assistance to Customer as requested by Customer.

6. SUB-PROCESSORS

6.1 Treasure Data is entitled to use Sub-processors for the purpose of providing the Service under the Agreement. Treasure Data provides information about its Sub-processors on its website (www.treasuredata.com/terms/) or otherwise in writing to Customer. Customer accepts Treasure Data's use of Sub-processors as they are listed on its website at the time of entering into the Service Agreement and as updated under this Clause 6. Treasure Data is entitled to reduce the number of Sub-processors without separate notice.

6.2 When adding a new Sub-processor: (i) Treasure Data shall update the list published on its website referred to under Clause 6.1 at least 30 days before the new Sub-processor Processes Personal Data under the Agreement. Such update is deemed to be a notice given to Customer about the proposed engagement of the new Sub-processor for the purpose of Clause 6.3 below; or (ii) Treasure Data shall notify Customer in writing pursuant to the provisions on legal notices under the Service Agreement about the proposed engagement of the new Sub-processor at least 30 days before the new Sub-processor Processes Personal Data under the Agreement.

6.3 Customer may object to Treasure Data's use of a new Sub-processor for Good Cause by notifying Treasure Data promptly in writing at legal@treasuredata.com within 14 days following notice of the new Sub-processor by Treasure Data. If Customer objects to a new Sub-Processor pursuant to this Clause 6.3, Treasure Data may make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the new Sub-processor without unreasonably burdening Customer. If Treasure Data confirms to Customer that Treasure Data is unable to make available such change, Customer may terminate, within 14 days of receiving such confirmation, only to that part of the Service which cannot be provided without the use of the new Sub-processor by providing written notice to Treasure Data at legal@treasuredata.com. "**Good Cause**" means a justified doubt as to whether the new Sub-processor can comply with the relevant contractual requirements described in this DPA. In the event Customer terminates the Service subscription pursuant to this Clause 6.3, Treasure Data will refund Customer any prepaid fees covering the remainder of the term of Service subscription following the effective date of termination with respect to such terminated Service without any further liability to Customer in respect of such termination.

6.4 If Customer does not object to the addition of a new Sub-Processor pursuant to Clause 6.3 or if, following any such objection, Customer does not terminate the Agreement pursuant to Clause 6.3, then Customer shall be deemed to have authorized Treasure Data to use the new Sub-processor.

6.5 Treasure Data shall ensure that its Sub-processors are subject to equivalent requirements regarding confidentiality and data protection as set out in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processors. Treasure Data remains responsible towards Customer for Treasure Data's Sub-processors' acts and omissions pursuant to the Agreement.

6.6 Where Standard Contractual Clauses apply between the Parties, Customer acknowledges and expressly agrees that pursuant to Clause 5(h) of the Standard Contractual Clauses, information about Treasure Data's Sub-processors is given as described in this Clause 6 and that Treasure Data may engage new Sub-processors as described in this Clause 6.

7. INTERNATIONAL TRANSFERS OF PERSONAL DATA

7.1 Customer acknowledges that the provision of the Service may require international transfers of Personal Data, including without limitation transfers to countries not recognized under Data Protection Legislation as providing an adequate level of protection of personal data. Customer hereby agrees to any such transfers, provided that Treasure Data complies with this Clause 7.

7.2 In respect of any transfer of Personal Data by Treasure Data under this DPA from the EEA, Switzerland or the UK to countries which do not ensure an adequate level of data protection (within the meaning of the applicable European Data Protection Legislation) and to the extent such transfers are subject to European Data Protection Legislation, Treasure Data will use at its discretion a permitted transfer mechanism under European Data Protection Legislation.

7.3 The Standard Contractual Clauses set out in Schedule 1 apply only in respect of those international transfers of Personal Data Processed under the Agreement that are subject to European Data Protection Legislation, as long as such law recognizes the Standard Contractual Clauses as a lawful transfer mechanism of Personal Data and only to the extent to which Treasure Data does not elect to use another permitted transfer mechanism under applicable European Data Protection Legislation ("**Relevant Transfer**").

7.4 Customer agrees that Treasure Data may transfer Personal Data if required to do so by law to which Treasure Data is subject; in such a case, Treasure Data shall inform Customer of such legal requirement before transfer, unless that law prohibits such information.

7.5 If Customer is not the Controller in respect of the Personal Data, then Customer is responsible for ensuring that its agreement with the Controller(s) allows for the use of all of the transfer mechanisms mentioned in this Clause 7. Customer warrants and represents that any relevant Controller has authorized Customer to agree to the transfers as described in this Clause 7.

8. AUDITS

8.1 Upon Customer's written request at reasonable intervals considering the circumstances, Treasure Data will make available to Customer such necessary information in Treasure Data's possession and control as Customer may reasonably request, with a view at demonstrating Treasure Data's compliance with the obligations of a Processor under the Data Protection Legislation in relation to Treasure Data's processing of Personal Data under this DPA.

8.2 Customer agrees to exercise any right it might have under applicable Data Protection Legislation to conduct an audit or an inspection by submitting a written request to Treasure Data for an audit report, in which case Treasure Data shall provide an audit report prepared by a respected third party which is not older than 12 months, in satisfaction of such request, so that Customer can reasonably verify Treasure Data's compliance with its obligations in relation to its Processing of Personal Data under this DPA.

8.3 Where the Standard Contractual Clauses apply between the Parties, the Parties agree that audits pursuant to Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses may be carried out as follows: (a) in accordance with Clauses 8.1 and 8.2 above of this DPA; and/or (b) Customer may contact Treasure Data to request an on-site audit of the procedures relevant to the protection of Personal Data and shall provide Treasure Data with at least 30 days prior written notice to prepare for the onsite audit. Customer shall reimburse Treasure Data for any time expended for any such on-site audit at Treasure Data's then-current professional services rates. Before the commencement of any such on-site audit, Customer and Treasure Data shall mutually agree upon the scope, timing, and duration of the audit in addition to the audit fee for which Customer shall be responsible. Customer shall promptly notify Treasure Data at security@treasure-data.com with information regarding any non-compliance discovered during the course of an audit.

8.4 Any information or audit report shared in accordance with this Clause 8 shall be Treasure Data's Confidential Information.

9. LIMITATION OF LIABILITY

Each Party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability set out in the Service Agreement.

10. TERM OF THE DPA AND CONSEQUENCES OF TERMINATION

10.1 This DPA shall continue in force until expiration or termination of the Service Agreement. Clauses 1, 2, 3.7, 9, 10 and 11 shall survive termination of this DPA.

10.2 Treasure Data shall, at Customer's choice, return or delete all Personal Data in its possession within 30 days from termination or expiration of the Service Agreement ("**Post-Termination Period**"), unless otherwise required by law. Where Customer elects to have Personal Data returned to it pursuant to this Clause 10.2, Treasure Data may fulfill its obligation under this Clause 10.2 by granting Customer, at Customer's cost and expense, access to Personal Data stored in the Service during the Post-Termination Period (or any other period as it may be agreed by the Parties in writing ("**Extended Post-termination Period**")) so as to allow Customer to extract a copy of the Personal Data. Where Personal Data are not deleted by Customer, Treasure Data shall delete Personal Data in its possession within the end of the Post-Termination Period or within 30 days from the expiration of the Extended Termination Period, unless otherwise required by law.

10.3 Where the Standard Contractual Clauses apply, the Parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Treasure Data to Customer upon Customer's written request.

11. CONFLICT RULES

Where the Standard Contractual Clauses at Schedule 1 apply, in the event of any conflict between Schedule 1 and any other provision of this DPA, Schedule 1 prevails.

12. AMENDMENTS TO THIS DPA

Treasure Data is permitted to modify this DPA, with updates to take effect only after the end of the applicable Subscription Term.

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES
Controller to Processor

Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

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 8.1(b), 8.9(a), (c), (d) and (e); (iii) Clause 9(a), (c), (d) and (e); (iv) Clause 12(a), (d) and (f); (v) Clause 13; (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); (viii) Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7 - Optional
Docking clause – Not Applicable

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.

Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[1] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (30) business 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[2]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10
Data subject rights

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

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

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

Clause 11
Redress

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

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

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to: (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; (ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12
Liability

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

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

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

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

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

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

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

Clause 13
Supervision

(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.

(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[3];

(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) (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 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 Ireland.

Clause 18
Choice of forum and jurisdiction

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

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

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

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

Appendix

ANNEX I

to the Standard Contractual Clauses

A. LIST OF PARTIES

Data exporter(s): The data exporter is Customer (as identified in this DPA).

Data importer(s): The data importer is Treasure Data (as identified in this DPA) which processes personal data upon the instructions of the data exporter pursuant to the Service Agreement and the DPA.

B. DESCRIPTION OF TRANSFER

Data subjects: As identified in Schedule 2 of the DPA in relation to the type(s) of services included in the Service.

Categories of data: As identified in Schedule 2 of the DPA in relation to the type(s) of services included in the Service.

Special categories of data: As identified in Schedule 2 of the DPA in relation to the type(s) of services included in the Service.

Processing operations: The objective of Processing of Personal Data by data importer is the performance of the Service pursuant to the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY (*Identify the competent supervisory authority/ies in accordance with Clause 13):*

The Data Protection Authority of ______________________.

ANNEX II

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

Data importer will maintain the administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Service referred to under clause 5 of the DPA between data exporter and data importer.

ANNEX III

LIST OF SUB-PROCESSORS

The current list of sub-processors for the Service is available at Treasure Data’s website: https://www.treasuredata.com/terms/

SCHEDULE 2

DETAILS OF THE SERVICE AND OF THE PROCESSING ACTIVITIES

Details of the Processing by Treasure Data in connection with the provision of Service**:**

Subject matter and duration of the Processing:	Provision of the Service to Customer; Treasure Data Processes Personal Data for as long as is necessary for the provision of the Service.
Nature and Purpose of Processing:	Treasure Data Processes Personal Data as necessary to perform the Service pursuant to the Agreement, and as it may be further specified in any technical documentation made available to Customer or further instructed by Customer pursuant to the Agreement in its use of the Service.
Types of Personal Data:	Personal Data may include but are not limited to: first and last name, job title, contact information (email, phone, business and/or home address), online unique identifiers, location data, browsing history, information about personal interests. *Special categories of Personal Data*: Subject to the restrictions set out in the Service Agreement, Customer may submit to the Service Personal Data which may consist of "special categories of personal data" (as this term is interpreted under the GDPR) provided that Customer complies with the applicable terms of the Data Protection Legislation governing such data.
Categories of Data Subjects	Categories of Data Subjects may include but are not limited to: natural persons who are prospects or customers of Customers, or users of Customers' products or services.

SCHEDULE 3

SECURITY MEASURES

1. Security Measures

Treasure Data's security measures are designed to: (a) ensure the security, integrity and confidentiality of Personal Data; (b) protect against reasonably anticipated threats or hazards to the security or integrity of Personal Data; and (c) protect against unauthorized access to or use of Personal Data that could result in substantial harm or inconvenience to the person that is the subject of Personal Data.

2. General Procedures

a. Data Storage. Personal Data is protected using cryptographic means when the interfaces to it cannot be properly enumerated and protected, such as when being transmitted over a network. When the data resides in a secure location, such as on servers that are adequately controlled, it is protected using logical means, such as: database access lists and file system permissions. When using cryptography, only established and/or NIST-approved algorithms and modes of operation are used; for example, symmetric encryption is done using AES-128 or AES-256, and transport encryption is carried out using TLS and DTLS. Personal Data that is stored on Internet-facing hosts is protected by network layer access control lists, which enforce a strict ruleset on incoming traffic. Anomalous activities, such as activities which can be indicative of an emerging attack, are logged and signaled for analysis and remediation.

b. Data Transfers. Treasure Data uses HTTPS standards to protect data integrity during transfers. In addition, subject to Clause 2.a above, Treasure Data will maintain at least the following security measures: HTTP with SSL 128-bit or 256-bit encryption (HTTPS); and secure access to the Service.

c. Access and Use Monitoring. Treasure Data will monitor Treasure Data's user access to and use of the Service for security, performance evaluation, and system utilization purposes.

3. Security reviews of the operations environment

The operations environment is repeatedly reviewed in design and actual execution. The latter is accomplished using penetration tests that are carried out by Treasure Data and external service providers. A summary of those reviews can be shared with Customer provided that the content may be redacted as necessary to ensure the confidentiality and security of the environment for other Treasure Data customers.

Treasure Data has experience in supporting external audits by third parties on behalf of customers. In such situations, some of the internal security review material can be shared with the external auditor to facilitate a more thorough review for lesser costs.

4. Network security

Network security is a wide security domain that is addressed at multiple levels, some of which are: (a) reliance on accredited and certified cloud providers to assure, inter alia, secure physical resources; (b) strong network layer access controls; (c) patch management and vulnerability management; (d) secure authentication supporting multiple robustness levels, according to the privilege of the account to which the user authenticates; (e) proper logging and signaling of both successful and failed attempts; (f) secure administrative remote access to the service network; and (f) proper utilization of key management mechanisms utilizing hardware and/or software.

5. Backup and Business Continuity

Treasure Data maintains a business continuity program, including a recovery plan, designed to ensure Treasure Data can continue to function and provide Service to Customer through an operational interruption. The program provides a framework and methodology, including a business impact analysis and risk assessment process, necessary to identify and prioritize critical business functions. If Treasure Data experiences an event requiring recovery of systems, information or services, the recovery plan will be executed promptly. Treasure Data continuously enhances the security and availability of its multi–tenant enterprise class cloud infrastructure.

6. Key Management

Encryption keys are used all around the hosted software application that are used to provide the Service. They are used for secure storage, secure transport, token generation, and authentication. The hosted software application used to provide the Service does not utilize a single centralized key-store for both architecture and security reasons. Different keys are stored by different means in accordance with their availability and security requirements.