# 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means all laws and regulations relating to the protection of personal data and privacy of individuals (amended, superseded or replaced from time to time), including without limitation the California Consumer Privacy Act, the GDPR, the European Directive 2002/58/EC (as amended by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applicable, the GDPR, the UK GDPR and the Federal Data Protection Act of 19 June 1992 (Switzerland), each as amended, superseded or replaced from time to time.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 the clauses included in Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87).

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@treasure-data.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 (PROCESSOR)

For the purposes of Article 26(2) of Directive 95/46/EC, respectively Articles 44 and 46 of the GDPR and Art. 6 of the Federal Data Protection Act of 19 June 1992 (Switzerland), for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Customer (as identified in the DPA to which this Schedule 2 is attached)

(the data **exporter**)

And

Name of the data importing organisation: Treasure Data (as identified in the DPA to which this Schedule 2 is attached)

(the data **importer**)

each a 'party'; together 'the parties',

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

***Clause 1***

*Definitions*

For the purposes of the Clauses:

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

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

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

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

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

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

***Clause 2***

*Details of the transfer*

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

***Clause 3***

*Third-party beneficiary clause*

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

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

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

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

***Clause 4***

*Obligations of the data exporter*

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

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

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

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

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

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

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

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

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

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

***Clause 5***

*Obligations of the data importer*

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

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

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

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

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

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

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

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

***Clause 6***

*Liability*

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

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

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor

agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

***Clause 7***

*Mediation and jurisdiction*

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

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

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

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

***Clause 8***

*Cooperation with supervisory authorities*

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

***Clause 9***

*Governing law*

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

***Clause 10***

*Variation of the contract*

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

***Clause 11***

*Sub-processing*

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

***Clause 12***

*Obligation after the termination of personal data-processing services*

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

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

**Appendix 1**

*to the Standard Contractual Clauses*

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

*Data exporter*

The data exporter is (please specify briefly your activities relevant to the transfer):

*Customer (as identified in the DPA).*

*Data importer*

The data importer is (please specify briefly activities relevant to the transfer):

*Treasure Data (as identified in the DPA) which processes personal data upon the instructions of the data exporter pursuant to the Service Agreement and the DPA.*

*Data subjects*

The personal data transferred concern the following categories of data subjects (please specify):

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

*Categories of data*

The personal data transferred concern the following categories of data (please specify):

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

*Special categories of data (if appropriate)*

The personal data transferred concern the following special categories of data (please specify):

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

*Processing operations*

The personal data transferred will be subject to the following basic processing activities (please specify):

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

**Appendix 2**

*to the Standard Contractual Clauses*

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

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.

## 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.<br><br>*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.