Data Processing Addendum

(including EU Standard Contractual Clauses)

This Data Processing Addendum ("DPA") and the schedules to this DPA apply to the Processing of Customer Personal Data on behalf of Customer as identified on the signature page in Section 18 (the "Customer") in order to provide Services Customer may have ordered from Census. This DPA forms part of the Terms of Service available at https://getcensus.com/terms-conditions or such other location as the Terms of Service may be posted from time-to-time or such alternative agreement Customer may have entered into with Census pursuant to which Customer has accessed Census's Services, as defined in the applicable agreement (the "Agreement"). In the event of a conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA will prevail, unless the Agreement explicitly provides otherwise, identifying the relevant portion of the DPA that it is superseding.

For purposes of this DPA, Customer and Census agree that Customer is the Data Controller of Customer Personal Data and Census is the Data Processor of such data, except when Customer acts as a Data Processor of Customer Personal Data, in which case Census is a subprocessor.

In the course of providing Services to Customer pursuant to the Agreement, Census may Process Customer Personal Data on behalf of Customer. Census agrees to comply with the following provisions with respect to any Customer Personal Data submitted by or on behalf of Customer for the Services or collected and Processed through the Services.

1. Definitions

Any capitalized term used but not defined in this DPA has the meaning provided to it in the Agreement or in the Applicable Data Protection Law.

a) "Applicable Data Protection Law" refers to all laws and regulations applicable to Census's Processing of Personal Data under the Agreement including, without limitation, the General Data Protection Regulation (EU 2016/679) ("GDPR").
b) "Customer Personal Data" means any Personal Data Processed by Census on behalf of Customer pursuant to or in connection with the Agreement.
c) "CCPA" means the California Consumer Privacy Act 2018 Cal. Civ. Code 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this Data Processing Addendum.
d) "Delete" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed, and "Deletion" will be construed accordingly.
e) "GDPR" means the EU General Data Protection Regulation 2016/679 and to the extent the GDPR is no longer applicable in the United Kingdom, any implementing legislation or legislation having equivalent effect in the United Kingdom. References to "Articles" or "Chapters" of the GDPR will be construed accordingly.

f) “Services” means those services and activities to be supplied to or carried out by or on behalf of Census for Customer pursuant to the Agreement.
g) “Transfer” means the transfer of Customer Personal Data outside the United Kingdom or EU/European Economic Area (“EEA”).
h) “Standard Contractual Clauses” means the standard contractual clauses issued by the European Commission for the transfer of Personal Data from Data Controllers established in the EU/EEA to Data Processors established outside the EU/EEA, currently in the form annexed to the European Commission’s decision of 5 February 2010 on Standard Contractual Clauses for the transfer of Personal Data to Data Processors established in third countries.
i) “Subprocessor” means any third party appointed by or on behalf of Census to Process Customer Personal Data.

2. Standard Contractual Clauses

Any Processing operations as described in Schedule 1 will be subject to this DPA which includes the Standard Contractual Clauses as contained in Schedule 2 whereby the Standard Contractual Clauses will prevail over any conflicting clauses in the Agreement or in this DPA, only when such Processing is subject to European Data Protection Law. The Parties agree that the Standard Contractual Clauses will be directly binding between Census as Data Importer (as defined therein) and Customer as Data Exporter (as defined therein) in relation to Customer Personal Data provided by Customer.

3. Processing of Customer Personal Data

Census will in the course of providing Services, including with regard to Transfers of Personal Data to a third country, Process Customer Personal Data only on behalf of and under the documented Instructions of Customer unless required to do so otherwise under Applicable Data Protection Law; in such a case, Census will inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Schedule 1 specifies the duration of the Processing, the nature and purpose of the Processing, and the types of Personal Data and categories of data subjects.

Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the Services and its own Processing of Customer Personal Data and (b) it has, and will continue to have, the right to Transfer, or provide access to, Customer Personal Data to Census for Processing in accordance with the terms of the Agreement and this DPA.

Customer appoints Census as a Data Processor to Process Customer Personal Data on behalf of, and in accordance with, Customer’s instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents and preventing spam or fraudulent activity, and detecting and preventing network exploits and abuse); (b) as necessary to comply with applicable law; and (c) as otherwise agreed in writing by the parties (“Permitted Purposes”).

Customer will ensure that its instructions comply with Applicable Data Protection Law. Customer acknowledges that Census is not responsible for determining which laws are applicable to Customer’s business nor whether Census’s provision of the Services meets or will meet the requirements of such laws. Customer will ensure that Census’s Processing of

Customer Personal Data, when done in accordance with Customer's instructions, will not cause Census to violate any applicable law, regulation, or rule, including Applicable Data Protection Law. Census will inform Customer if it becomes aware or reasonably believes that Customer's data Processing instructions violate any applicable law, regulation, or rule, including Applicable Data Protection Law.

Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or Processing, or prior to permitting Customer's end users to transmit or Process, any Special Categories of Data via the Services.

Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Customer Personal Data, to the extent applicable under the CCPA.

4. Security

Census will ensure that its employees (including subprocessors) who Process Customer Personal Data for Census or who have access to Customer Personal Data are authorized to Process this Personal Data, and have undertaken to, or are contractually bound to observe confidentiality. Census will ensure that this obligation to maintain confidentiality continues beyond the termination of employment contracts or service contracts, and beyond the termination of this DPA.

Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Natural Persons, Census will in relation to Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR. As appropriate, this may include:

- the pseudonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; and
- the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident.

In assessing the appropriate level of security, Census will take into account the risks presented by Processing, in particular from a Personal Data Breach. Census's technical and organizational measures specified in Schedule 2 Appendix 2 are subject to technical advancements and development. Census will regularly test, assess and evaluate the effectiveness of technical and organizational measures to reasonably ensure the security of the Processing.

5. Subprocessing

Customer agrees that Census may use subprocessors to fulfill its contractual obligations under the Agreement. Where Census authorizes any subprocessor as described in this Section 5, Census agrees to impose data protection terms on any subprocessor it appoints that require it to protect Customer Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate

technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR.

Customer provides a general consent for Census to engage onward subprocessors, conditional on the following requirements:

a. Any onward subprocessor must agree in writing to only Process data in a country that the European Commission has declared to have an “adequate” level of protection; or to only Process data on terms equivalent to the Standard Contractual Clauses, or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities; and
b. Census will restrict the onward subprocessor’s access to Customer Personal Data only to what is strictly necessary to provide the Services, and Census will prohibit the subprocessor from Processing the Customer Personal Data for any other purpose.

Customer consents to Census engaging additional third party subprocessors to Process Customer Personal Data within the Services for the Permitted Purposes provided that Census maintains an up-to-date list of its subprocessors at https://getcensus.com/census-subprocessors. Census will provide details of any change in subprocessors as soon as reasonably practicable, but in any event will give notice no less than fourteen (14) days prior to any such change.

The Customer may object to the new or changed Subprocessor within five calendar days after receipt of Census’s notice. If within five (5) calendar days of receipt of that notice, Customer notifies Census of an objection to an appointment (based on reasonable grounds relating to data protection), then (i) Census will work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and (ii) where such a change cannot be made within fourteen (14) days from Census’s receipt of Customer’s objection notice, notwithstanding anything in the Agreement, Customer may, by such notice to Census, terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor. Such termination will be without prejudice to any fees incurred by Customer prior to suspension or termination. If no objection has been raised prior to Census replacing or appointing a new subprocessor, Census will deem Customer to have authorized the new subprocessor.

Census will remain liable for any breach of this DPA that is caused by its subprocessors.

6. Data Rights Requests

Census’s Services provide Customer with a number of self-service features, including the ability to rectify, delete, obtain a copy of, or restrict use of Customer Personal Data, which may be used by Customer to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to requests from data subjects via the Census Services at no additional cost. In addition, upon Customer’s request, Census will provide reasonable additional and timely assistance (at Customer’s expense only if complying with Customer’s request will require Census to assign significant resources to that effort) to assist Customer in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory or third party, including, but not limited to law enforcement, is made directly to Census in connection with Census’s Processing of Customer Personal Data, Census will

inform Customer providing details of the same, to the extent legally permitted. Unless legally obligated to do so, Census will respond to any such request, inquiry or complaint without Customer's prior consent. In the case of a legal demand for disclosure of Customer Personal Data in the form of a subpoena, search warrant, court order or other compulsory disclosure request, Census will attempt to redirect the requesting party or agency to request disclosure from Customer. If Census is legally compelled to respond to such a request, Census will notify Customer prior to disclosure of Customer Personal Data so that Customer may seek a protective order or other relief, if appropriate, unless Census is barred by law from giving such notification.

7. Personal Data Breach

Upon becoming aware of a Personal Data Breach, Census will without undue delay and within (72) seventy-two hours inform Customer and provide written details of the Personal Data Breach reasonably required to fulfill Customer's notification obligations under Applicable Data Protection Law. Where possible, such details will include, the nature of the Personal Data Breach, the categories and approximate number of data subjects concerned and the categories and approximate number of Customer Personal Data records concerned, the likely consequences, and the measures taken or proposed to be taken to mitigate any possible adverse effects.

Census will promptly work to recover Customer Personal Data which is lost, damaged, destroyed or distorted as a result of the Personal Data Breach, and take such reasonable commercial steps as may be directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. DPIA and Consultation

Census will provide reasonable assistance to Customer in connection with data protection impact assessments, and prior consultations with Supervisory Authorities, which Customer reasonably considers to be required of Customer by Article 35 or 36 of the GDPR, with regards to Processing of Customer Personal Data by Census.

9. Return and Deletion of Customer Personal Data

Within one (1) month after the expiry or termination of the Agreement, Census will, upon Customer's request return all Customer Personal Data to Customer, by providing access via the Census Services, and will destroy any Customer Personal Data and any copies in Census's control or possession and as required by applicable law and provide written confirmation once returned or destroyed.

Census may retain Customer Personal Data after the expiry or termination of the Agreement to the extent required by applicable law, and only to the extent and for such period as required by applicable laws and always provided that Census will ensure the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

10. De-Identified Data

"De-identified Data" means Customer Personal Data that has been Processed such it can no longer be linked to an identified or identifiable Natural Person, or a device linked to such person.

Census may Process Customer Personal Data to create de-identified data for Census's legitimate business purposes. De-identified data will not be considered Customer Personal Data and Census may retain such data at its discretion.

11. Audits

Census will make available information to Customer at Customer's request which is necessary to demonstrate compliance with this DPA and allow for any audits, including inspections, conducted by Customer or another auditor, as requested by Customer on reasonable, legitimate grounds for suspecting a breach of this DPA. Census will provide for such audits by allowing Customer to review confidential summary reports ("Audit Report") prepared by third-party security professionals at Census's selection and Expense.

If Customer can demonstrate that it requires additional information, beyond the Audit Report, then Customer may request, at Customer's cost, Census to provide for an audit subject to reasonable confidentiality procedures, which will: (i) not include access to any information that could compromise confidential information relating to other Census customers or suppliers, Census's technical and organizational measures or any trade secrets; and (ii) be performed upon no less than sixty (60) days' notice, during regular business hours and in such a manner as not to unreasonably interfere with Census's normal business activities. If Census is unable to follow Customer's instructions (for example, where Customer's request relates to a subprocessor that will not provide such information or right to Census) or declines, Customer may terminate the Agreement.

12. International Data Transfers

Customer authorizes Census and its subprocessors to Transfer Customer Personal Data across international borders, including from the UK or European Economic Area to the United States. Any international Transfer of Customer Personal Data from the UK or European Economic Area to a Third Country must be supported by an approved EU adequacy mechanism.

Census and Customer will use the Standard Contractual Clauses in Schedule 2 as the adequacy mechanism supporting the Transfer and Processing of Customer Personal Data.

13. Jurisdiction Specific Terms

Where Census Processes Customer Personal Data protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 3, the terms specified in Schedule 3 with respect to the applicable jurisdiction(s) ("Jurisdiction Specific Terms") apply in addition to the terms of this DPA. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this DPA, the applicable Jurisdiction Specific Terms will take precedence.

14. Liability

Customer and Census will each be separately liable to the other party for damages it causes by any breach of the clauses in this DPA. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party will be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its Applicable Data Protection Law.

15. Failure to Perform.

In the event that changes in law or regulation render performance of this DPA impossible or commercially unreasonable, the Parties may renegotiate this DPA in good faith. If renegotiation would not cure the impossibility, or the Parties cannot reach an agreement, the Parties may terminate the Agreement in accordance with the Agreement's termination provisions.

16. Updates

Census may update the terms of this DPA from time to time; provided, however, Census will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) the release of new products or services or material changes to any of the existing Services; (b) changes in Applicable Data Protection Law; or (c) a merger, acquisition, or other similar transaction. The then-current terms of this DPA are available at https://getcensus.com/security.

17. Duration and Survival

This DPA will become legally binding upon the Effective Date of the Agreement or upon the date that the Parties sign this DPA if it is completed after the effective date of the Agreement. Census will Process Customer Personal Data until the relationship terminates as specified in the Agreement. Any obligation imposed on Census under this DPA in relation to the Processing of Customer Personal Data will terminate when Census no longer Processes Customer Personal Data.

18. Signature Page

SIGNED FOR AND ON BEHALF OF Census	SIGNED FOR AND ON BEHALF OF CUSTOMER
Company Name:	Company Name:
Sutro Labs, Inc. (dba Census)	
……...	……...
Signature:	Signature:
……	……
Name: Boris Jabes	Name:
……	……
Position: CEO	Position:
……	……
Date: 1st February 2021	Date:
……	……

Schedule 1

Customer Personal Data Processing Details

Subject Matter of Processing	The Processing will involve: • the performance of the Services pursuant to the Agreement.
Duration of Processing	The Processing will continue as set forth in the Agreement.
Categories of Data Subjects	• Customer employees, contractors, agents, and/or representatives • Customer's customers and affiliates, and their employees, contractors, agents, representatives, and customers (some of which may be end users of Customer's products and services) • Any other category of Data Subject that Customer is a Data Controller or Data Processor of that Customer chooses to Process within the Services.
Special Categories of Personal Data	Sensitive data as provided by Customer for Processing within the Services including but not limited to government ID numbers, date of birth, financial account information, health information and/or information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, health, and sex life.
Nature and Purpose of Processing	Includes the following: The Processing activities performed by Census will be as described in the Agreement.
Types of Personal Data	• Standard contact information such as name, title, email address, physical address, phone number, etc. • Information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location
Census subprocessor list	https://getcensus.com/census-subprocessors

Schedule 2

EU Standard Contractual Clauses (Processors)

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

Customer is hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by the respective Data Exporter.
Census is hereinafter referred to as the "**Data Importer**".

The Data Exporter and the Data Importer, each a “party” and collectively “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 **Schedule 1**.

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

(g) '*Addendum'* has the meaning given to it in the Background recital above.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which

shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the 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

Subprocessing

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

Clause 12

Obligation after the termination of personal data processing services

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

On behalf of the data exporter (Customer):

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

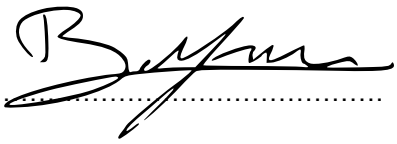
On behalf of the data importer (Census):

Name (written out in full): Boris Jabes

Position: CEO

Address: 340 S Lemon Ave #1097, Walnut, CA 91789, United States

Other information necessary in order for the contract to be binding (if any):

Signature… 

Appendix 1 to the Standard Contractual Clauses

This Appendix 1 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 1.

Data exporter

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

- The Data Exporter is the Customer of Census's Services as defined in the Agreement.

Data importer

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

- The Data Importer is Census which offers services to Customer through its online platform with respect to the Services.

Data subjects

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

- See Schedule 1 of the DPA.

Categories of data

The Personal Data transferred concern the following categories of data subjects (please specify, tick the applicable):

- See Schedule 1 of the DPA.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify, tick the applicable):

- See Schedule 1 of the DPA.

Processing operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify):

- See Schedule 1 of the DPA.

On behalf of the data exporter (Customer):

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……

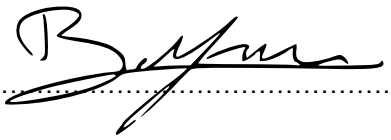
On behalf of the data importer (Census):

Name (written out in full): Boris Jabes

Position: CEO

Address: 340 S Lemon Ave #1097, Walnut, CA 91789, United States

Other information necessary in order for the contract to be binding (if any):

Signature…… 

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 Organizational Security Measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

This information is located at https://getcensus.com/security/.

On behalf of the data exporter (Customer):

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……

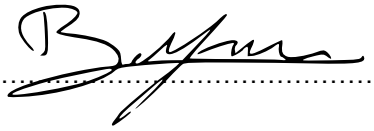
On behalf of the data importer (Census):

Name (written out in full): Boris Jabes

Position: CEO

Address: 340 S Lemon Ave #1097, Walnut, CA 91789, United States

Other information necessary in order for the contract to be binding (if any):

Signature…… 

Schedule 3

Jurisdiction Specific Terms

Canada:

1.1. The definition of “Applicable Data Protection Law” includes The Federal Personal Information Protection and Electronic Documents Act (PIPEDA).

1.2. Census’s subprocessors, as described in Schedule 1 of this DPA, are third parties under Applicable Data Protection Law, with whom Census has entered into a written contract that includes terms substantially similar to this DPA. Census has conducted appropriate due diligence on its subprocessors.

1.3. Census will implement technical and organizational measures as set forth in Section 4 (Security) of this DPA.

United Kingdom:

2.1 References in this DPA to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018)

2.2 The Standard Contractual Clauses will also apply to Customer in the United Kingdom as data exporter and to Census as data importer for Transfers of Personal Data to countries that are not deemed to have an adequate level of data protection under the United Kingdom's Applicable Data Protection Law.

United States - California:

3.1 The definition of “Applicable Data Protection Law” includes the California Consumer Privacy Act of 2018 (CCPA).

3.2 The definition of “Data Controller” includes “Business” as defined under Applicable Data Protection Law.

3.3 The definition of “Data Processor” includes “Service Provider” as defined under Applicable Data Protection Law.

3.4 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law and, for clarity, includes any Personal Information contained within Customer Personal Data.

3.5 The definition of “Data Subject” includes “Consumer” as defined under Applicable Data Protection Law. Any Data Subject rights, as described in Section 6 (Data Rights Requests) of this DPA, apply to Consumer rights.

3.6 Census will Process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Census agrees not to (a) sell (as defined by the CCPA) Customer’s Personal Data or Customer end users’ Personal Data; (b) retain, use, or disclose Customer’s Personal Data for any

commercial purpose (as defined by the CCPA) other than providing the Services; or (c) retain, use, or disclose Customer's Personal Data outside of the scope of the Agreement.

3.7 Census certifies that its subprocessors, as listed in Schedule 1 of this DPA, are Service Providers under Applicable Data Protection Law, with whom Census has entered into a written contract that includes terms substantially similar to this DPA. Census conducts appropriate due diligence on its subprocessors.

3.8 Census will implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Data it Processes as set forth in Section 4 (Security) of this DPA.