

Census

Data Processing Addendum

Schedule 1 – Data Processing Terms

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.

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) and UK 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 the UK GDPR. 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 European Economic Area (“EEA”).
- h) “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

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.

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. Appendix 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 fraudulent activity); (b) as necessary to comply with Applicable Data Protection 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 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://www.getcensus.com/list-of-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 (48) forty-eight 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. 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.

11. 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 EEA to a Third Country must be supported by an approved Cross Border Transfer Mechanism.

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

12. 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.

13. 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.

14. 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.

15. 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>.

16. 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.

17. 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: 21st September 2022

Date:

.....

.....

Appendix 1

Customer Personal Data Processing Details

Subject Matter of Processing	The Processing will involve: <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 identifiers 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://www.getcensus.com/list-of-subprocessors

Appendix 2 - Technical and Organizational Security Measures

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, Processor shall implement the measures outlined at <https://getcensus.com/security> to ensure an appropriate level of security for the provision of the Services.

Where applicable, this Appendix 2 will serve as Annex II to the Standard Contractual Clauses.

Schedule 2 - Cross Border Transfer Mechanisms

1. Definitions

- “EC” means the European Commission
- “EEA” means the European Economic Area
- ”Standard Contractual Clauses” means, depending on the circumstances unique to Customer, any of the following:
 - a) EU Standard Contractual Clauses, and
 - b) UK International Data Transfer Agreement
- "EU Standard Contractual Clauses" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- “UK International Data Transfer Agreement” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1 Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Customer Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2; (b) the UK International Data Transfer Agreement as set forth in Section 2.3 (UK International Data Transfer Agreement) of this Schedule 2; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2 EU Standard Contractual Clauses. The parties agree that the EU Standard Contractual Clauses will apply to Customer Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA Area that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

- (a) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Customer Personal Data and Census is processing Customer Personal Data.

(b) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Personal Data and Census is processing Customer Personal Data.

(c) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of subprocessor changes will be as set forth in Section 5 (Subprocessing) of this DPA;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

(v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the EU Standard Contractual Clauses:

- Data Exporter: Customer.
- Contact Details: The email address(es) designated by Customer in Customer's account via its notification preferences.
- Data Exporter Role: The Data Exporter's role is set forth in Section 3 (Processing of Customer Personal Data) of this DPA.
- Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
- Data Importer: Sutro Labs, Inc. (dba Census)
- Contact details: Census Privacy Team – privacy@getcensus.com.
- Data Importer Role: Data Processor.

- Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) in Annex I, Part B of the EU Standard Contractual Clauses:

- The categories of data subjects are described in Appendix 1 (Customer Personal Data Processing Details) of this DPA.
- The Sensitive Information transferred is described in Appendix 1 (Customer Personal Data Processing Details) of this DPA.
- The frequency of the transfer is a continuous basis for the duration of the Agreement.
- The nature of the processing is described in Appendix 1 (Customer Personal Data Processing Details) of this DPA.
- The purpose of the processing is described in Appendix 1 (Customer Personal Data Processing Details) of this DPA.
- The period for which the Customer Personal Data will be retained is described in Appendix 1 (Customer Personal Data Processing Details) of this DPA.
- For transfers to subprocessors, the subject matter, nature, and duration of the processing is set forth at <https://www.getcensus.com/list-of-subprocessors>.

(viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Appendix 2 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

2.3 UK International Data Transfer Agreement. The parties agree that the UK International Data Transfer Agreement will apply to Customer Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Customer Personal Data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information are located in Section 2.2 (c)(vi) of this Schedule 2.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2.

(c) In Table 3 of the UK International Data Transfer Agreement:

1. The list of Parties is located in Section 2.2(c)(vi) of this Schedule 2.
2. The description of the transfer is set forth in Appendix 1 (Customer Personal Data Processing Details) of this DPA.
3. Annex II is located in Appendix 2 (Technical and Organizational Security Measures) of this DPA.
4. The list of sub-processors is located at <https://www.getcensus.com/list-of-subprocessors>.

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.4 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, including Schedule 3 (Jurisdiction Specific Terms), or the Agreement, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.

Schedule 3

Jurisdiction Specific Terms

1. Australia:

1.1 The definition of “Applicable Data Protection Law” includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

1.3 The definition of “Sensitive Information” includes “Sensitive Information” as defined under Applicable Data Protection Law.

2. Brazil:

2.1 The definition of “Applicable Data Protection Law” includes the Lei Geral de Proteção de Dados (LGPD).

2.2 The definition of “Security Breach” includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of “processor” includes “operator” as defined under Applicable Data Protection Law.

3. California:

3.1 The definition of “Applicable Data Protection Law” includes the California Consumer Privacy Act (CCPA) and, beginning January 1, 2023, the California Privacy Rights Act (CPRA).

3.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

3.3 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, include any Consumer rights. In regards to Data Subject requests, Census can only verify a request from Customer and not from Customer’s end user or any third party.

3.4 The definition of “controller” includes “Business” as defined under Applicable Data Protection Law.

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

3.6 Census will process, retain, use, and disclose Customer 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) the Customer Personal Data; (b) retain, use, or disclose the Customer Personal Data for any commercial purpose (as defined by the CCPA) or other purpose other than for the specific purpose of providing the Services; or (c) retain, use, or disclose Customer Personal Data outside of the direct business relationship between the parties as set forth in the Agreement. Additionally, beginning January 1, 2023, Census: (a) shall not share (as defined in the CPRA) Customer Personal Data; (b) shall not combine Customer Personal Data with other Personal Information (as defined in the CPRA) received from any other source, except as otherwise permitted by the CPRA or its regulations; (c) shall provide the same level of privacy protection as is required by the CPRA; (d) shall notify Customer promptly in writing if Census makes a determination that it can no longer meet its obligations under the CPRA; (e) grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate Census’s unauthorized use of Customer Personal Data and to take reasonable and appropriate steps to ensure that Census uses the Customer Personal Data in a manner consistent with Customer’s CPRA obligations. Census certifies that it understands its obligations under Applicable Data Protection Law and this Section 3.6 and will comply with them.

3.7 Census certifies that its subprocessors, as described in Section 5 (Subprocessing) 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 Customer Personal Data it processes to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure as set forth in Section 4 (Security) of this DPA.

4. Canada:

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

4.2 Census’s subprocessors, as described in Section 5 (Subprocessing) 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.

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

5. European Economic Area (EEA):

5.1 The definition of “Applicable Data Protection Law” includes the General Data Protection Regulation (EU 2016/679) (“*GDPR*”).

5.2 When Census engages a subprocessor under Section 5 (Subprocessing) of this DPA, it will:

(a) require any appointed subprocessor to protect the 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, and

(b) require any appointed subprocessor to (i) agree in writing to only process Customer Personal Data in a country that the European Union has declared to have an “adequate” level of protection or (ii) only process Customer Personal Data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

5.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the GDPR.

6. Israel:

6.1 The definition of “Applicable Data Protection Law” includes the Protection of Privacy Law (PPL).

6.2 The definition of “controller” includes “Database Owner” as defined under Applicable Data Protection Law.

6.3 The definition of “processor” includes “Holder” as defined under Applicable Data Protection Law.

6.4 Census will require that any personnel authorized to process Customer Personal Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Census in accordance with Section 4 (Security) of this DPA.

6.5 Census must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 4 (Security) of this DPA and complying with the terms of the Agreement.

6.6 Census must ensure that the Customer Personal Data will not be transferred to a subprocessor unless such subprocessor has executed an agreement with Census pursuant to Section 5 (Subprocessing) of this DPA.

7. Japan:

7.1 The definition of “Applicable Data Protection Law” includes the Act on the Protection of Personal Information (APPI).

7.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

7.3 The definition of “controller” includes “Business Operator” as defined under Applicable Data Protection Law. As a Business Operator, Census is responsible for the handling of Customer Personal Data in its possession.

7.4 The definition of “processor” includes a business operator entrusted by the Business Operator with the handling of Customer Personal Data in whole or in part (also a “trustee”), as described under Applicable Data Protection Law. As a trustee, Census will ensure that the use of the entrusted Customer Personal Data is securely controlled.

8. Mexico:

8.1 The definition of “Applicable Data Protection Law” includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).

8.2 When acting as a processor, Census will:

(a) treat Customer Personal Data in accordance with Customer’s instructions set forth in Section 3 (Processing of Customer Personal Data) of this DPA;

(b) process Customer Personal Data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Applicable Data Protection Law and Section 4 (Security) of this DPA;

(d) keep confidentiality regarding the Customer Personal Data processed in accordance with the Agreement;

(e) delete all Customer Personal Data upon termination of the Agreement; and

(f) only transfer Customer Personal Data to subprocessors in accordance with Section 5 (Subprocessing) of this DPA.

9. Singapore:

9.1 The definition of “Applicable Data Protection Law” includes the Personal Data Protection Act 2012 (PDPA).

9.2 Census will process Customer Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 4 (Security) of this DPA and complying with the terms of the Agreement.

10. Switzerland:

10.1 The definition of “Applicable Data Protection Law” includes the Swiss Federal Act on Data Protection.

10.2 When Census engages a subprocessor under Section 5 (Subprocessing) of this DPA, it will:

(a) require any appointed subprocessor to protect the 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, and

(b) require any appointed subprocessor to (i) agree in writing to only process Customer Personal Data in a country that the European Union has declared to have an “adequate” level of protection or (ii) only process Customer Personal Data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

11. United Kingdom (UK):

11.1 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).

11.2 When Census engages a subprocessor under Section 5 (Subprocessing) of this DPA, it will:

(a) require any appointed subprocessor to protect the 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; and

(b) require any appointed subprocessor to (i) agree in writing to only process Customer Personal Data in a country that the United Kingdom has declared to have an “adequate” level of protection or (ii) only process Customer Personal Data on terms equivalent to the UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

11.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the UK GDPR.