Instructions to customer for signing Mapbox DPA:

- Page 6: Please fill in your legal entity name and other required information and sign.
- Page 22: Please fill in the required information and sign.
- Page 24: Please fill in the Competent Supervisory Authority that applies to your business, depending on whether you are established or not established or have appointed a representative in the EU.

Data Processing Addendum

This Data Processing Agreement ("**DPA**") is made and entered into effective as of the later of the dates signed by a Party hereto ("**Effective Date**").

Between:

The company set forth below on the signature page below ("**Customer**"); and

Mapbox, Inc. ("**Mapbox**"), a company constituted under the laws of Delaware with an address of 740 15th Street NW, 5th Floor, Washington DC 20005

(together, the "**Parties**" and the "**Party**" shall be construed accordingly).

Recitals

A. Mapbox is the provider of the Services, as defined in the agreement by and between the Parties ("**Agreement**").

B. Mapbox may from time to time process certain personal data or personal information identified on **Schedule B** ("**Customer Data**") on behalf of Customer to enable Mapbox to provide the Services to Customer in accordance with the Agreement ("**Purpose**") and Customer may make Customer Data available to Mapbox in connection with this Purpose.

C. This DPA forms part of the Agreement to reflect the Parties' agreement with regard to the processing of Customer Data.

D. The Parties intend that the processing activities carried out by Mapbox on behalf of Customer shall comply with the provisions of this DPA.

1. Definitions

Words and expressions used in this DPA but not defined herein shall have the meanings given to such words and expressions in the General Data Protection Regulation (2016/679) ("**GDPR**") or the Agreement.

"**Standard Contractual Clauses**" means the standard contractual clauses set out in the European Commission's decision (EU) 2019/914of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Collectively, the GDPR and the California Consumer Privacy Act of 2018 ("**CCPA**") shall be referred to "**Applicable Data Protection Law**".

2. Details of the Processing Operations

The subject matter of the processing, including the processing operations carried out by Mapbox on behalf of Customer are described in Schedule B, which forms an integral part of this DPA. Mapbox acts on behalf of and on the instructions of Customer, as described in the Agreement, in carrying out the processing operations.

3. Obligations of Customer

3.1. Customer determines the purposes for which Customer Data are being or will be processed and the manner in which they are being or will be processed.

3.2. Customer represents, warrants and agrees that with respect to Customer Data provided to Mapbox pursuant to this DPA, Customer:

3.2.1. complies with personal data security and other obligations prescribed by Applicable Data Protection Law;

3.2.2. confirms that the provision of Customer Data to Mapbox complies with Applicable Data Protection Law;

3.2.3. has established a procedure for the exercise of the rights of the individuals whose Customer Data are collected;

3.2.4. only processes data that have been lawfully and validly collected and ensures that such data is relevant and proportionate to the respective uses;

3.2.5. ensures that after assessment of the requirements of Applicable Data Protection Law, the security and confidentiality measures implemented are suitable for protection of Customer Data against any accidental or unlawful destruction, accidental loss, alteration, unauthorized or unlawful disclosure or access, in particular when the processing involves data transmission over a network, and against any other forms of unlawful or unauthorized processing; and

3.2.6. takes reasonable steps to ensure compliance with the provisions of this DPA by its personnel and by any person accessing or using Customer Data on its behalf.

4. Obligations of Mapbox

4.1. Mapbox carries out the processing of Customer Data on behalf of Customer.

4.2. Mapbox agrees to provide Customer Data with at least the same level of protection as required under the Standard Contractual Clauses. Mapbox further agrees to only process Customer Data (i) in furtherance of the Purpose, and (ii) in accordance with the Agreement, this DPA and the Standard Contractual Clauses.

4.3. Mapbox agrees that it will:

4.3.1. not sell Customer Data;

4.3.2. adhere to the requirements of Article 28 of GDPR;

4.3.3. process Customer Data only on behalf of Customer and in compliance with Customer's written instructions, as specified in this DPA and the Agreement, unless required to do so by EU, Member State or local law to which Mapbox is subject;

4.3.4. if in Mapbox's opinion an instruction from Customer infringes Applicable Data Protection Law, promptly inform Customer;

4.3.5. implement the technical and organizational security measures provided for in **Schedule C** prior to the commencement of the processing activities for Customer Data, maintain such security measures (or security measures that are not materially less protective) for the duration of this DPA, and provide Customer with reasonable evidence of its privacy and security policies upon request;

4.3.6. take reasonable steps to ensure that (i) persons employed by it and (ii) other persons engaged at its place of business who may process Customer Data comply with this DPA;

4.3.7. comply with confidentiality obligations in respect of Customer Data (as specified in the Agreement) and take reasonable steps to ensure that its employees, authorized agents and any sub-processors comply with such confidentiality obligations;

4.3.8. inform Customer of:

4.3.8.1. any legally binding request for disclosure of Customer Data by a law enforcement authority, to the extent permitted by law and legal process, such as in order to preserve the confidentiality of an investigation by the law enforcement authorities;

4.3.8.2. any personal data breach within the meaning of Applicable Data Protection Law relating to Customer Data which would require a notification to be made to a supervisory authority or data subject under Applicable Data Protection Law;

4.3.8.3. any relevant notice, inquiry or investigation by a supervisory authority relating to Customer Data, to the extent permitted by applicable law and legal process; and

4.3.8.4. any requests for access to, rectification or blocking of Customer Data received directly from a data subject prior to responding to that request, unless Customer has authorized a response or such a response is required by law;

4.3.9. provide reasonable co-operation and assistance to Customer in respect of Customer's obligations regarding:

4.3.9.1. requests from data subjects in respect of access to or the rectification, erasure, restriction, blocking or deletion of Customer Data;

4.3.9.2. the investigation of any personal data breach within the meaning of Applicable Data Protection Law relating to Customer Data and the notification to the supervisory authority and data subjects in respect of such a personal data breach;

4.3.9.3. the preparation of data protection impact assessments and, where applicable, carrying out consultations with the supervisory authority;

4.3.9.4. the security of Customer Data, including by implementing the technical and organizational security measures provided for in Schedule C;

4.3.10. if Mapbox is required by law to process Customer Data to which GDPR applies, take reasonable steps to inform Customer of this requirement in advance of any processing, unless Mapbox is prohibited from informing Customer on grounds of important public interest; and

4.3.11. upon reasonable request, make available to Customer information reasonably necessary to demonstrate compliance with the obligations in this section 4. All such information shall be provided subject to a strict duty of confidentiality.

4.4. Mapbox agrees at the request of Customer to submit to an audit to ascertain and/or monitor Mapbox's compliance with this DPA and Applicable Data Protection Law which audit shall be carried out no more than once in any 12 month period (unless otherwise required by a supervisory authority) for cause with reasonable notice and during regular business hours and in a manner which is not disruptive to Mapbox's business and under a duty of confidentiality, by one of the 'big 4' auditing firms appointed by Customer and accepted by Mapbox. The scope of such an audit will be agreed in advance and shall not involve physical access to the network and hosting infrastructure on which the Services are hosted. Customer hereby agrees that an audit may only be conducted if necessary to prove facts which Mapbox cannot verify by providing Customer with independent evidence, including evidence of its compliance with a third party certification programme. Customer will bear its own costs, the fees of any auditor and any expenses incurred by Mapbox in complying with this section 4.4 and section 4.3.9. This paragraph only applies to the extent expressly required under Applicable Data Protection Law.

5. Transfer, Disclosure and Third Parties

Mapbox may engage third parties acting on its behalf to assist in satisfying its obligations in accordance with this DPA and to delegate all or part of the processing activities to such sub-processors. Mapbox shall enter into contractual arrangements with such sub-processors requiring them to guarantee a similar level of data protection compliance and information security to that provided for herein. For the purposes of this Section 5, Customer hereby consents to Mapbox engaging sub-processors. Mapbox shall maintain a current list of its sub-processors with respect to Customer Data, access to which can be provided to Customer, and which information shall be held by Customer as strictly confidential and only used to enforce its rights under this Section 5. Customer may object to changes concerning the engagement or replacement of a sub-processor but only on reasonable and documented grounds relating to the protection of Customer Data. Such an objection must be given by notifying Mapbox promptly in writing, within 5 business days after Mapbox updates its sub-processor list, explaining reasonable grounds for the objection. In the event Customer objects to a new sub-processor, as permitted in the preceding sentence, Mapbox shall have the right to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of personal data by the objected-to new sub-processor. If Mapbox is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days (the "**Cure Period**"), either party may terminate without penalty by either party that part of the Services which cannot be provided by Mapbox without the use of the objected-to new sub-processor by providing written notice to the other party within 5 business days after the end of the Cure Period.

6. Post-termination Obligations

During the term of the Agreement, Customer can use the functionality provided to access and download uploaded data. Upon expiration or termination of Customer's relationship with Mapbox, Mapbox will delete all Customer Data in accordance with its standard deletion policy unless applicable EU, Member State or local law prevents it from destroying all or part of Customer Data. In such case, Mapbox agrees to preserve the confidentiality of Customer Data retained by it and that it will only actively process such Customer Data after such date in order to comply with the laws it is subject to.

7. International Data Transfers

For transfers of personal data under this DPA from the European Union, the European Economic Area and/or their member states, the United Kingdom and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Applicable Data Protection Laws of the foregoing territories, the Standard Contractual Clauses set forth in Schedule D to this DPA shall apply.

8. Disclaimer

To the fullest extent permissible pursuant to applicable law, Mapbox disclaims all warranties not expressly set out in the Agreement and this DPA. In particular, Mapbox does not warrant that Customer Data will continue to be stored, will continued to be available or will not become corrupted.

9. Governing Law and Jurisdiction

The governing law, venue, and dispute resolution provisions of the Agreement shall apply to this DPA.

10. Conflict

In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail.

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

CUSTOMER		**MAPBOX**	
Legal Entity:	_____		
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Schedule A

Additional Data Transfer Terms

1. Additional Terms to Standard Contractual Clauses

1.1. **Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of execution of the DPA for the processing of personal data. Any additional or alternate instructions must be agreed upon separately in writing and signed by both parties. For the purposes of Clause 8.1 of the Standard Contractual Clauses, the processing described in Section 2 of the DPA ("Details of the Processing Operations") is deemed an instruction by the Customer to process personal data.

1.2. **Appointment of new sub-processors and list of current sub-processors.** Pursuant to Clause 9(a) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Mapbox will appoint sub-processors in accordance with Section 5 of the DPA ("Transfer, Disclosure and Third Parties"). In accordance with Section 5 of the DPA, Mapbox shall make available to Customer the current list of sub-processors at https://www.mapbox.com/legal/subprocessors.

1.3. **Notification of new sub-processors and Objection Right for new sub-processors.** Pursuant to Clause 9(a) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Mapbox may engage new sub-processors as described in Section 5 of the DPA. In the event that Mapbox is required to complete an emergency change of sub-processor, Mapbox agrees to inform Customer of an emergency change of sub-processor as soon as is reasonably practicable before or after such a change occurs.

1.4. **Copies of sub-processor Agreements.** The parties agree that the copies of the sub-processor agreements that must be provided by Mapbox to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Mapbox beforehand; and, that such copies will be provided by Mapbox, in a manner to be determined in its discretion, only upon request by Customer.

1.5. **Audits and Certifications.** The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 4.4 of the DPA.

1.6. **Certification of Deletion.** The parties agree that the certification of deletion of personal data that is described in Clause 16(d) of the Standard Contractual Clauses shall be provided by Mapbox to Customer only upon Customer's request.

1.7. **Conflict.** In the event of any conflict or inconsistency between the body of the DPA, this Schedule, and any of its Schedules, and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

1.8. **Non-receipt of directives under FISA Section 702 rep:** Mapbox represents and warrants that, as of the effective date of the DPA, it has not received any national security orders of the type described in Paragraphs 150-202 of the

judgment in the European Court of Justice Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*").

1.9. **FISA Section 702:** Mapbox may be eligible to be required to provide information, facilities, or assistance under Section 702 of the Foreign Intelligence Surveillance Act ("**FISA**") as:

- an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4). However, Mapbox has never received a process issued under FISA Section 702 for services it provides to its customers.
- However, Mapbox is not the type of provider that is eligible to be subject to upstream collection ("bulk" collection) pursuant to FISA Section 702, as described in paragraphs 62 & 179 of the *Schrems II* judgment.

1.10. **Court-review safeguard:** Should Mapbox receive demands for data access through national security process for data related to customer or its end users, Mapbox shall use commercially reasonable legal mechanisms to challenge such demands as well as any non-disclosure provisions attached thereto.

1.11. **Notice of demand:** To the extent legally permissible, Mapbox shall promptly notify the data exporter if it receives demands for data access through national security process for data related to customer or its end users and shall make all reasonable legal efforts to refrain from providing data until customer has had an opportunity to challenge any demands.

1.12. **EO 12333 non-cooperation:** Mapbox shall take no action pursuant to U.S. Executive Order 12333.

In the event of any conflict or inconsistency between this Schedule and the Clauses, then the Clauses shall prevail.

Schedule B

Details of the Processing Activities

Data subjects

The Customer Data transferred concern the following categories of data subjects or consumers:

- personal data or personal information that is contained in "Your Uploads" (as defined in the Agreement) (if any).

Categories of data

The Customer Data transferred is:

- personal data or personal information comprised in "Your Uploads" meaning data which is uploaded by Customer to Mapbox via Mapbox Studio, Mapbox Studio Classic, our Dataset API, Tilesets API or our Upload API so that Mapbox can host it for Customer as part of providing our Services.

Special categories of data

Customer is not permitted to submit special categories of personal data to Mapbox through the Services, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, health and/or sex life.

Processing operations

The Customer Data transferred may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and improve the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement.

Schedule C

Technical and Organisational Security Measures

In accordance with section 4 of the DPA, Mapbox will adopt and maintain reasonable (including organisational and technical) security measures in dealing with Customer Data in order to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In determining the technical and organizational security measures required by section 4 of the DPA, Mapbox will take account of 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.

Mapbox will implement the following specific security measures, as applicable:

- The security measures detailed at: https://www.mapbox.com/platform/security/ as amended from time to time.

Schedule D

STANDARD CONTRACTUAL CLAUSES

Section I

Clause 1

Purpose and scope

The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(1) The Parties:

- the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
- the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(2) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(3) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

A. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

B. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

1.1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

1.2. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

1.5. Clause 13;

1.6. Clause 15.1(c), (d) and (e);

1.7. Clause 16(e);

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

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

Clause 4

Interpretation

- Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

Intentionally
Omitted.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer

shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter

"sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object

to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

Clause 11

Redress

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

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with

these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers;

the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation . The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

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

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

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

APPENDIX
ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses:

   Signature and date: …

   Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: **Mapbox, Inc.**

   Address: **740 15th Street NW, 5th Floor, Washington DC 20005**

   Contact person's name, position and contact details: legal@mapbox.com

   Activities relevant to the data transferred under these Clauses: See Appendix B.

   Signature and date: ……..

   Role (controller/processor): **Processor**

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

The Customer Data transferred concern the following categories of data subjects or consumers:

- personal data or personal information that is contained in "Your Uploads" (as defined in the Agreement) (if any).

Categories of personal data transferred

The Customer Data transferred is:

- personal data or personal information comprised in "Your Uploads" meaning data which is uploaded by Customer to Mapbox via Mapbox Studio, Mapbox Studio Classic, our Dataset API, Tilesets API or our Upload API so that Mapbox can host it for Customer as part of providing our Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The Customer is not permitted to submit special categories of personal data to Mapbox through the Services, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, health and/or sex life.

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

The data is transferred on a continuous basis.

Nature of the processing

The Customer Data transferred may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and improve the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement.

Purpose(s) of the data transfer and further processing

The Customer Data is processed for the following purposes:

- storage necessary to provide, maintain and improve the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement.

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

Customer Data will be retained (i) for the period such Customer Data is actively in use by Customer as part of Customer's use of the Services and/or (ii) until Mapbox has received a valid deletion request from Customer.

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

The subject matter, nature, and duration of processing by sub-processors is identical to that of processing by Mapbox since sub-processors are integral to our provision of online services.

……..

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

_____

…….

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Mapbox will adopt and maintain reasonable (including organisational and technical) security measures in dealing with Customer Data in order to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In determining the technical and organizational security measures, Mapbox will take account of 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.

Mapbox will implement the following specific security measures, as applicable:

- The security measures detailed at: https://www.mapbox.com/platform/security/ as amended from time to time.