Legal

Last Updated February 1, 2023

Data Processing Addendum

Addendum

This Data Processing Addendum (**"DPA"**) is incorporated into and forms part of the Master Services Agreement (**"Agreement"**) entered into by and between Customer and Mixpanel, Inc. (**"Mixpanel"**) (collectively the **"Parties"**), pursuant to which Customer has subscribed to Mixpanel's Application Services as defined in the applicable Agreement. The purpose of this DPA is to reflect the Parties' agreement regarding Processing Personal Data in accordance with the Data Protection Legislation.

In the course of providing the Application Services to Customer pursuant to the Agreement, Mixpanel may Process Personal Data on behalf of Customer. The Parties agree to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Application Services or collected and Processed by or for Customer through the Application Services. Any capitalized but undefined terms herein shall have the meaning set forth in the Agreement.

Definitions

"**Data Protection Legislation**" means, as applicable, the Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (**"GDPR"**), the United Kingdom Data Protection Act 2018, the United Kingdom's General Data Protection Regulation (as incorporated under the European Withdrawal Act of 2018 as amended by the Data Protection, Privacy and Electronic Communications Regulation of 2019) that implements the GDPR ("**UK-GDPR**"), the United Kingdom's Privacy and Electronic Communications Regulation of 2003 (**"PECR"**), the Swiss Federal Act on Data Protection of 1992 (as amended) (**"FADP"**); the Virginia Consumer Data Protection Act; from and after July 31, 2023, the Colorado Privacy Act and the regulations promulgated thereunder, and Connecticut's Act Concerning Personal Data Use; Online Monitoring; and from and after December 31, 2023, the Utah Consumer Privacy Act; and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction.

"Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

"**Controller**," "**Processor**," "**Data Subject**," "**Personal Data**," "Process", "**Processing**," and "**Appropriate Technical and Organisational Measures**" shall be interpreted in accordance with applicable Data Protection Legislation;

"**Subprocessor**" or "**Sub-processor**" means any person (including any third party and any Mixpanel Affiliate, but excluding Mixpanel personnel) appointed by or on behalf of Mixpanel or any Mixpanel Affiliate to Process Personal Data on behalf of Customer and/or Customer Affiliate in connection with the Agreement.

Data Protection Terms

Relationship of the Parties. The Parties agree that Customer is the Controller and that Mixpanel is its Processor in relation to Personal Data that is Processed by Mixpanel in the course of providing the Application Services. Customer shall comply at all times with Data Protection Legislation in respect of all Personal Data it provides to Mixpanel pursuant to the Agreement and in connection with its use of the Application Services.

Customer Affiliates. If a Customer Affiliate has executed an Ordering Document, but is not itself a party to the Agreement, this DPA is an addendum to that Ordering Document. If a Customer Affiliate is neither a party to an Ordering Document nor the Agreement, this DPA does not apply to that Affiliate. Such an Affiliate should request that the Customer execute a data processing agreement for the benefit of that entity.

Purpose, Duration, and Nature of Processing. The subject matter of the Processing covered by this DPA is the license to access and use the Application Services ordered by Customer either through Mixpanel's website or through an Ordering Document and provided by Mixpanel to Customer via www.mixpanel.com, or as additionally described in the Agreement, Ordering Document, or this DPA. The Processing will be carried out until the term listed in the applicable Ordering Document ceases. Details on the nature of the Processing are set out in Schedule 1 to this DPA.

Processing Requirements. In respect of Personal Data Processed by Mixpanel in the course of providing the Application Services, Mixpanel:

1. Shall Process Personal Data: (i) in accordance with the documented instructions from Customer as set out in this DPA, the Agreement, or (if applicable) the Ordering Document; (ii) shared or transmitted by Customer in connection with Customer's use of the Application Services; and (iii) to comply with other written, reasonable instructions provided by Customer where such instructions are consistent with the terms of this DPA, the Agreement, and Data Protection Legislation. If Mixpanel is required to Process Personal Data for any other purpose provided by applicable law to which it is subject, Mixpanel will inform Customer of such requirement prior to the Processing unless that law prohibits this on important grounds of public interest;

2. Shall notify Customer without undue delay if, in Mixpanel's opinion, an instruction for the Processing of Personal Data provided by Customer through the Application Services infringes applicable Data Protection Legislation;

3. Shall, without limitation of Customer's security obligations under the Agreement, implement and maintain Appropriate Technical and Organisational Measures designed to protect Personal Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure, or access. These measures shall be designed to provide a level of security appropriate to the risk of harm which might result from such incidents and having regard to the nature of the Personal Data which is to be protected;

4. May hire and has hired other companies to provide limited services on its behalf, provided that Mixpanel complies with the provisions of this clause. Customer hereby confirms its general authorization for Mixpanel's use of Subprocessors. Mixpanel's current Subprocessors list is available at: https://mixpanel.com/legal/subprocessor-list/ (the "**Authorized Subprocessors**"). The Subprocessors will be permitted to Process Personal Data only to deliver the services Mixpanel has retained them to provide, and they shall be prohibited from using Personal Data for any other purpose. Mixpanel remains responsible for its Subprocessors' compliance with the obligations of this DPA. Any Subprocessors to whom Mixpanel transfers Personal Data will have entered into written agreements with Mixpanel requiring that the Subprocessor abide by terms consistent with the requirements of this DPA. At least thirty (30) days prior to the date on which any new Subprocessor shall commence Processing Personal Data, Mixpanel will update the list of Authorized Subprocessors to include the new Subprocessor. If Customer would like to receive notification of such an update to the list, Customer may sign up to receive such notice by emailing compliance@mixpanel.com. If Customer has a legitimate objection to Mixpanel's appointment of a new Subprocessor, Customer may notify Mixpanel in writing by emailing compliance@mixpanel.com within fourteen (14) calendar days of receiving the notice. Legitimate objections must contain reasonable and documented grounds relating to a Subprocessor's non-compliance with applicable Data Protection Legislation. If, in Mixpanel's reasonable opinion, such objections are legitimate, the Customer may, by providing written notice to Mixpanel, terminate the Agreement. Customer acknowledges and agrees that (a) Mixpanel's Affiliates may be retained as Subprocessors through written agreement with Mixpanel and (b) Mixpanel and Mixpanel Affiliates respectively may engage third party subcontractors, pursuant to this clause 4, in connection with the provision of the Application Services;

5. Shall ensure that all Mixpanel personnel required to access the Personal Data are informed of the confidential nature of the Personal Data, are subject to a duty of confidentiality in respect thereof, and comply with the obligations set out in this DPA and applicable Data Protection Legislation;

6. Shall, at Customer's written request, assist the Customer by implementing appropriate and reasonable technical and organisational measures to assist with the Customer's obligation to respond to requests from Data Subjects to exercise rights under Data Protection Legislation (including requests for information relating to the Processing, and requests relating to access, rectification, erasure or portability of Personal Data) provided that Mixpanel reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance;

7. Shall take reasonable steps at the Customer's request to assist Customer in meeting Customer's obligations under Article 32 to 36 of the GDPR taking into account the nature of the Processing under this DPA; provided, however, that Mixpanel reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance;

8. Shall, at the end of the applicable term of the Application Services and upon Customer's written request, securely destroy or return such Personal Data to Customer, unless retention is required by law, and, if requested by Customer, provide Customer with information necessary to demonstrate compliance with this obligation;

9. Agrees, where Mixpanel Processes or permits any Subprocessor to Process Personal Data in any country not deemed to provide an adequate level of protection of Personal Data by Data Protection Legislation, to transfer such Personal Data across international borders as follows: (i) for the European Union and the European Economic Area in compliance with the Standard Contractual Clauses which shall be incorporated in full by reference and form an integral part of this DPA, and which are set forth in Schedule 2 below ("**Standard Contractual Clauses**" or "**SCCs**"), provided that in the event of a conflict between the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall control, (ii) for the United Kingdom, in compliance with the Standard Contractual Clauses as amended in accordance with guidance from the United Kingdom's Information Commissioner's Office as set forth in Schedule 3; and (iii) for Switzerland, in compliance with the Standard Contractual Clauses as amended in accordance with guidance from the Federal Data Protection and Information Commissioner as set forth in Schedule 4 which the Parties agree shall apply to such transfer;

10. Shall, upon written request, either provide information regarding its compliance in the form of third-party certifications and audits reports on its security, privacy and architecture or respond with industry standard written audit questionnaires, provided that the purpose of such audit is to verify that Mixpanel is Processing Personal Data in accordance with its obligations under the DPA. Such audit may be carried out by Customer or an inspection body composed of independent members and in possession of required professional certificates or qualifications that bind said body to a duty of confidentiality, and for the avoidance of doubt, no access to any part of Mixpanel's information technology systems, data hosting sites or centers, or its infrastructure will be permitted. Only to the extent that such audit of Mixpanel's third-party certifications, audit reports and/or industry standard written audit questionnaires cannot reasonably demonstrate Mixpanel's compliance with its obligations under the DPA, may Customer or an inspection body composed of independent members elected by Customer that is bound by a duty of confidentiality conduct an on-site audit of Mixpanel. Any on-site audit rights of Customer will not include access to any Subprocessor's facilities. Any on-site audit shall: (i) be conducted at the expense of Customer; (ii) be conducted under mutually agreed notice, scope and duration; (iii) exclude any internal accounting or financial information, trade secret, data or information of any other Mixpanel customer (including its end users), or any information that in Mixpanel's reasonable opinion could compromise the security of its systems or premises or cause Mixpanel to be in breach of its obligations under Data Protection Legislation or its security, confidentiality, or privacy obligations to any other Mixpanel customer or third-party; and (iv) be limited to once per calendar year. The Parties agree that any audit described in the Standard Contractual Clauses shall be performed pursuant to this provision;

11. Shall notify Customer without undue delay if Mixpanel becomes aware of a breach of its security leading to any accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to Personal Data that is Processed by Mixpanel in the course of providing the Application Services (**"Incident"**) under the Agreement and provide Customer (as soon as possible thereafter) with a description of the Incident as well as periodic updates to information about the Incident, including its impact on Personal Data. Mixpanel shall additionally take action to investigate the Incident and reasonably prevent or mitigate the effects of the Incident; and

12. Shall provide relevant information reasonably requested by Customer to demonstrate compliance with the obligations set out in this DPA.

Limitation of Liability. This DPA shall be subject to the limitations of liability agreed between Customer and Mixpanel in the Agreement and such limitation shall apply in aggregate for all claims under the Agreement and DPA.

Incorporation and Precedence. This DPA is hereby incorporated into and forms part of the Agreement. In the event of any conflict or inconsistency between this DPA and the Agreement or, if applicable, an order form governed by the Agreement (an "**Ordering**

Document") and any such individually negotiated agreement or addendum, this DPA shall prevail, unless otherwise explicitly specified in an Ordering Document. In the event of any conflict or inconsistency between any SCCs entered into pursuant to this DPA, the Agreement and/or an Ordering Document, the SCCs shall prevail.

DPA Schedule 1

Details of the Data Processing

Nature and Purpose of Processing

Mixpanel Processes Personal Data to provide the Application Services pursuant to the Agreement and the DPA. Mixpanel Processes Personal Data sent by Customer's end users identified through Customer's implementation of the Application Services. As an example, in a standard programmatic implementation, to utilize the Application Services, Customer may allow the following information to be sent by default as "default properties":

Types of Personal Data

- City
- Region
- Country
- Time zone
- Browser
- Browser Version Device
- Current URL Initial Referrer
- Initial Referring Domain Operating System Mixpanel Library Referrer
- Referring Domain Screen Height Screen Width Search Engine Search Keyword
- UTM Parameters (i.e., any UTM tags associated with the link a customer clicked to arrive at the domain)
- Last Seen (the last time a property was set or updated).

For a full list of default properties available to Customer, see: https://mixpanel.com/help/questions/articles/what-properties-do-mixpanels-libraries-store-by-default.

Categories of Data Subjects

Users of the Customer's web and mobile applications.

DPA Schedule 2

Standard Contractual Clauses (Processors)

For the purposes of Article 28 and Article 46 of the GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

In keeping with those provisions, Mixpanel, Inc. shall be deemed the "Data Importer" and Customer shall be deemed the "Data Exporter." The Data Importer's contact information is as follows:

Name: Mixpanel, Inc.
Address: One Front Street, 28th Floor, San Francisco, CA 94111
Email: compliance@mixpanel.com

The Data Exporter's contact information appears on the applicable Order Form, Invoice, or Master Service Agreement between Customer and Mixpanel.

The Data Exporter and the Data Importer HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the Personal Data identified in either the Agreement or Schedule 1 to the DPA.

Section I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
- (iii) Clause 9(a), (c), (d) and (e);
- (iv) Clause 12(a), (d), and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

This Clause Purposely 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.

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 benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) (the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION. 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

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

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

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

Clause 11

Redress

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

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

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

- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
- (ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

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

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

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

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

importer's responsibility for the damage.

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

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

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

Clause 13

Supervision

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

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

(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

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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

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

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

Standard Contractual Clauses

Annex I

A. LIST OF PARTIES

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]

The Data Exporter is the entity identified as “Customer” or “Controller” in the Agreement.

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

The Data Importer is Mixpanel, Inc. (**"Mixpanel"**), a company providing hosted business software applications that processes personal data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The Personal Data transferred concern the categories of Data Subjects defined in Schedule 1 to the DPA.

Categories of personal data transferred

The Personal Data transferred concern the categories of data defined in Schedule 1 to the DPA.

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.

n/a

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

Continuous

Nature of the processing

The provision of services under the Agreement by Mixpanel to Customer

Purpose(s) of the data transfer and further processing

For Mixpanel to provide the services under the Agreement to Customer

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

Unless otherwise required by applicable law, the personal data may be retained by the Data Importer for a period ending upon the earlier of (i) the duration of services under the Agreement, or (ii) as determined by the Data Exporter.

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

Please see Annex III (List of Sub-processors)

C. COMPETENT SUPERVISORY AUTHORITY

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

Where the Data Exporter is established in a European Economic Area country and processes the contemplated personal data in the context of its establishment, the supervisory authority is the one of this European Economic Area country (Art 3.1 of the GDPR).

Where the Data Exporter is not established in a European Economic Area country but falls within the scope of the GDPR on an extra territorial basis (Art 3.2 of the GDPR):

- Where it has appointed an EU representative (Art 27 of the GDPR), the supervisory authority is the one of the European Economic Area countries in which the Data Exporter's representative is located;
- Where it does not have to appoint an EU representative, the supervisory authority is that of one of the European Economic Area country in which the data subjects whose data are being transferred pursuant to these Standard Contractual Clauses are located.

Standard Contractual Clauses

Annex II

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

The Data Importer's Technical and Organisational Measures described at: https://mixpanel.com/legal/tom/ describes the technical and organisational security measures that Data Importer has implemented.

Standard Contractual Clauses

Annex III

List of Subprocessors

Subprocessors. For the purposes of Clause 9 of these Clauses, the Data Exporter hereby consents to the Data Importer subcontracting any or all of its data processing operations performed under these Clauses to the extent permitted and in accordance with the DPA. Further, the Parties agree that for the purpose of Clause 9:

- (i) The list of approved Sub-processors is available at: https://mixpanel.com/legal/subprocessor-list/; and
- (ii) To receive notification of updates to the list of Subprocessors, Data Exporter must first submit a request for such notifications in writing to Mixpanel by emailing compliance@mixpanel.com. Data Importer will then provide Data Exporter with updates to such Subprocessor list (if any) in accordance with the DPA.

Data Subject Requests. For the purpose of Clause 10(a) of the Clauses, the Data Exporter hereby authorizes the Data Importer to respond to Data Subject requests received directly by Data Importer from Data Subjects to inform the Data Subject that (i) it is in receipt of the complaint, inquiry or request, (ii) it has notified the data controller of the same, and (iii) it is awaiting further instruction from the data controller.

DPA Schedule 3

UK Addendum to Standard Contractual Clauses (Processors)

International Transfer Agreement

This UK Addendum to Standard Contractual Clauses (Processors) International Transfer Agreement ("**Addendum**") has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Table 1: Parties

Start Date: The Effective Date of the Agreement

The Parties	Exporter who sends the Restricted Transfer	Importer who receives the Restricted Transfer
Parties' Details	Customer	Mixpanel, Inc.
Key Contact	Attn: Customer email: electronic mail address provided for Customer's account owner	Attn: General Counsel email: compliance@mixpanel.com

Table 2: Selected SCCs, Modules and Selected Clauses

Selected SCCs, Modules and Selected Clauses	Contents
Addendum EU SCC	The version of the Approved EU SCCs which this Addendum is appended to, detailed below: Module 2, as set out in Schedule 2 to the DPA.
Module	Module 2, as set out in Schedule 2 to the DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendices of the Approved EU SCCs as incorporated by reference into the DPA and set forth in Schedule 2 of the DPA.

Annexes	Contents
Annex 1A	List of Parties: As set out in the Agreement.
Annex 1B	Description of Transfer: As set out in Schedule 1 to the DPA.
Annex II	Technical and organizational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II to the SCCs.
Annex III*	List of subprocessors: As set out in Annex III to the SCCs.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum Changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer (yes) ☐ Exporter (yes) ☐ neither Party (no)

Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

DPA Schedule 4

Swiss Addendum to Standard Contractual Clauses (Processors)

Insofar as the data transfer under the DPA is governed by the FADP, provided that none of these amendments will have the effect or be construed to amend the Standard Contractual Clauses in relation to the processing of Personal Data under to the GDPR, the following shall apply:

1. the Swiss Federal Data Protection and Information Commissioner (the **"FDPIC"**) will be the competent supervisory authority, in Annex I.C under Clause 13 of the SCCs;
2. the applicable law for contractual claims and place of jurisdiction for actions between the Parties under Clauses 17 and 18 of the SCCs shall be as set forth in the SCCs, provided that that the term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs;
3. references to the "GDPR" should be understood as references to the "FADP;" and
4. where the FADP protects legal entities as Data Subjects, the SCCs will apply to data relating to identified or identifiable legal entities.

;
;