

## DATA PROCESSING AGREEMENT

### Addendum

This Data Processing Addendum (the “DPA”) supersedes and replaces that certain Data Protection Addendum executed between Mixpanel, Inc. (“Mixpanel”) and PagoPA S.p.A. (the “Customer”) (collectively, the “Parties”) on or about March 31, 2020, and forms part of the Mixpanel Master Services Agreement executed by the Parties concurrently with this DPA (the “Agreement”).

### Background

On or around March 31, 2020, Mixpanel and Customer entered into a relationship whereby Customer retained Mixpanel to Process certain Personal Data on its behalf and in accordance with its instructions.

Since March 31, 2020, Customer and Mixpanel have amended and revised their prior Data Protection Addendum on several occasions to better reflect Customer’s instructions and Mixpanel’s Processing activities in response to those instructions.

The Parties have now decided to consolidate those instructions into this DPA that shall supersede and replace the prior Data Protection Addendum.

As with the prior Data Protection Addendum, this DPA reflects the Parties’ mutual agreement and commitment to Processing Personal Data in accordance with the General Data Protection Regulation and other applicable data protection legislation (as defined below).

Now there, and while providing the Application Services to Customer under the Agreement, Customer will entrust Mixpanel to Process Personal Data on Customer’s behalf pursuant to Article 28 of the General Data Protection Regulation. Mixpanel agrees to act as Customer’s Processor, and 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.

### Definitions

Any capitalized but undefined terms herein shall have the meaning set forth in the Agreement.

“**Data Protection Legislation**” means the Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (the “**GDPR**”), 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. For the purposes of this DPA, Affiliate shall also mean any third party, including any authorized resellers, that purchase the Application Services on behalf and/or to the benefit of the Customer.

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

“**Data Residency Program**” means Mixpanel’s storage and processing of data in the Google Cloud Platform’s “Europe-west4” data center in Eamshaven, Netherlands.

“Subprocessor” or “Sub-processor” means any person (including any third party and any Mixpanel Affiliate, but excluding an employee of Mixpanel or any of its subcontractors) entrusted by or appointed 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

- a) Relationship of the Parties. The Parties agree that Customer may act, as the Data Controller or Data Processor, as the case may be, and that Mixpanel is its Data Processor (or Sub-Processor) in relation to Personal Data that is Processed while providing the Application Services. Mixpanel shall have no right to store, use or access Customer Content or Personal Data for any purpose other than complying with Customer’s instructions as set forth in the Agreement and this DPA. Customer shall always comply 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.
- b) 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.
- c) 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 through an Ordering Document and provided by Mixpanel to Customer via [www.mixpanel.com](http://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 Annex 1 to this DPA.
- d) Data Residency Certification and Transfers. Mixpanel hereby certifies and affirms that Customer participates in Mixpanel’s Data Residency Program, and that all data sent by Customer to Mixpanel is stored and Processed in the European Union. In two circumstances, Mixpanel may process Customer data in the United States: (1) to provide support services to the Customer in response to a request from the Customer and (2) to provide debugging or maintenance of Mixpanel’s application, cloud infrastructure, or computing resources. For the avoidance of any doubt, processing activities outside the European Union may occur (i) in the United States only, excluding any transfer in any third country, (ii) for the specific purposes under (1) and (2) in this subsection d), (iii) by Mixpanel or through its Sub-processors located or operating in the United States (or such country identified in Annex 5) authorised by Customer according to Clauses 8.8 and 9 of Annexes 2 and 3, and to Annex 5 to this DPA.
- e) Prior to the execution of this DPA, the Parties conducted the assessment provided by Clause 14 of the SCCs (“**Transfer Impact Assessment**”) and concluded that the laws and practices of the United States, along with the safeguards put in place by Mixpanel, do not in practice prevent the Parties from fulfilling their obligations under the SCCs with regard to transfers of personal data outside of the EU, and are compatible with the commitments required by Article 46 of the GDPR regarding the transfer tools. As long as Processing of Personal Data by Mixpanel while providing the Application Services implies a transfer of such Personal Data, as authorised by Customer in accordance with this DPA, the Parties agree to maintain and update the Transfer Impact Assessment.
- f) Order of Precedence. For the avoidance of doubt, Mixpanel and Customer agree that, to the extent the terms of this DPA conflict with the Agreement or any Ordering Document, the DPA shall control for all purposes related to the collection, processing, storage, transmission, or use of Personal Data.
- g) Third Party Access Requests. Without prejudice to Clause 15 of the Standard Contractual Clauses, from time to time, and upon Customer’s written request, Mixpanel shall provide an Attestation Regarding Third Party Access. Such Attestation shall confirm whether or not Mixpanel received any third-party request for access to Customer Content or Customer Controlled Personal Data.
- h) 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.

- [REDACTED]
- i) Data Retention. Mixpanel shall only retain Personal Data Processed under this DPA for the period required by Customer. Customer shall retain the ability to set the data retention period in accordance with Customer's internal policies and the Data Protection Legislation.
  - j) Governing Law; Venue. Section 12.1 of the Agreement applies.
  - k) Processing Requirements. In respect of Personal Data Processed while 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 implement and maintain Appropriate Technical and Organisational Measures designed to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the Personal Data which is to be protected;
  4. Shall notify Customer in writing 30 (thirty) days before appointing new sub-processors or subcontractors for Processing Personal Data. Customer shall promptly review such appointment in good faith and lodge any objections to such appointment in writing to Mixpanel. If Customer does not object to the appointment within 30 days, Mixpanel shall treat such non-objection as approval of the appointment. If Customer objects to the appointment, Customer must provide written support for the objection and provide such other information as Mixpanel may reasonably request. Solely in the case Mixpanel cannot provide the Service (as defined in the Agreement) without use of the objectionable sub-processor or subcontractor, Customer may terminate the Agreement;
  5. Shall ensure that all Mixpanel personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations sets out in this clause 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 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;
9. Agrees, where Mixpanel Processes or permits any Subprocessor, in accordance with letter d) of the Data Protection Terms of this DPA, 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 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 Annexes 2 and 3 below, provided that in the event of a conflict between the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall control;
10. Upon written request, shall 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. 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. The Parties agree that any audit described in the Standard Contractual Clauses shall be performed pursuant to this provision; and
11. Shall notify Customer within twenty-four (24) hours of becoming 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 while providing the Application Services (an "Incident") under the Agreement. In the event of an Incident, Mixpanel will provide Customer with a description of the Incident as well as periodic updates about the Incident as such information becomes available to Mixpanel, including providing any information Mixpanel develops regarding the potential impact of such an Incident on Data Subjects. Mixpanel shall take reasonable action to investigate the Incident and take steps to reasonably mitigate the effects of the Incident and prevent its recurrence. Mixpanel shall also provide relevant information to Customer so Customer may demonstrate its compliance with Data Protection Legislation and this DPA.
12. **Compliance with Article 30 of GDPR (Records of Processing Activities); Ultimate Controllers.** The Parties agree, in their respective capacities, to maintain a record of all processing activities related to Customer's use of Mixpanel's Application Services in compliance with Article 30 of GDPR ("**Article 30 Records**").

Where Customer acts as a processor, pursuant to its responsibilities under Article 64-bis of the Legislative Decree 7 March 2005, n. 82 and subsequent amendments, the Parties agree that for the purposes of the processing carried out by Mixpanel on behalf of the Customer is in capacity of a processor of other controllers ("**Ultimate Controller**") as identified in the list notified from time to time to Mixpanel:

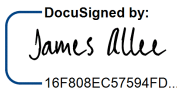
- **Article 30 Records.** In its Article 30 Records, Mixpanel shall refer to Customer's Ultimate Controllers as identified in the list notified from time to time to Mixpanel in writing by Customer;
- **Authorisation to Process.** Customer instructs and shall have obtained sufficient authorization from the Ultimate Controller to instruct Mixpanel to Process Ultimate Controller Personal Data to provide the Application Services under the Agreement and

as reasonably necessary to enable Mixpanel to comply with the instructions provided by Customer on behalf of the Ultimate Controller.

- **Transfer.** As it relates to the transfer of Customer Content, Customer is the Exporter and Mixpanel the Data Importer, whether based on direct or onward transfer, and Annex 2 (“Standard Contractual Clauses (Controller to Processors)”) or Annex 3 to the DPA (“Standard Contractual Clauses (Processor to Processor)”) shall apply, as the case may be.
- **Data Subject Requests. Point of Contact.** Customer hereby authorizes Mixpanel, and has obtained sufficient authorization from the Ultimate Controller to allow Mixpanel (where it is not appropriate for Customer to directly respond to data subjects), to respond to data subject requests related to Customer’s use of the Application Services received directly by Mixpanel, according to the reasonable instructions given by Customer from time to time also on behalf of the Ultimate Controllers. Customer has obtained from the Ultimate Controllers the authorization to be designated as the exclusive point of contact for notice purposes under any Data Protection Legislation provision regulating notices to controllers (including notices related to data subject requests specified in Clause 10(a) of the Standard Contractual Clauses).

IN WITNESS WHEREOF, the Parties' authorized signatories have duly executed this Agreement as of the Effective Date:

MIXPANEL, INC.

By (Signature):   
16F808EC57594FD...

Name (Printed): James Allie

Title: General Counsel

Date: 12/1/2022

CUSTOMER:

By (Signature):

Name (Printed):

Title:

Date:

Firmato digitalmente da: MARTA COLONNA  
Data: 14/12/2022 17:05:21



## DPA Annex 1

### *Details of the Data Processing*

Mixpanel shall process information to provide the Application Services pursuant to the Agreement and the DPA. Mixpanel shall process information sent by Customer's End Users, as defined in the Agreement, identified through Customer's implementation of the Application Services. **Types of Personal Data**

1. Categories of personal data include navigation, diagnostic and usage data related to Customer's services and products, unique identifiers and other Personal Data that Customer may submit through the Application Services the extent of which is determined and controlled by Customer in its sole discretion.
2. Some diagnostic events related to sensitive personal data (e.g. diagnostic data related to EU Covid Certificates) may be processed for public interest purposes and for a limited period of time, as applicable in relation to events collected and exclusively determined by the exporter in its sole discretion for its institutional tasks

### **Categories of Data Subjects**

Customer's End Users.

### **Processing Activities**

The processing activities necessary to provide the Application Services to Customer under the Agreement and the DPA.

## DPA Annex 2

### *Standard Contractual Clauses (Controller to Processor)*

#### **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) (1) 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) and (d);
  - (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 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.

##### **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 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**

- (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 thirty (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. (8) 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; or

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; or

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 (12);
  - (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 [for Module Three: the controller or] 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:
  - (iii) 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;
  - (iv) the data importer is in substantial or persistent breach of these Clauses; or
  - (v) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
- (d) 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. 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 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 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

##### Data exporter(s):

Name: PagoPA S.p.A.

Address: Piazza Colonna 370, CAP 00187, Roma, Italy (seat) - Via Sardegna 38, CAP 00187 (HQ)

Contact person's name, position and contact details: Marta Colonna, DPO, dpo@pagopa.it

Activities relevant to the data transferred under these Clauses: provision of Application Services by importer to exporter.

Signature and date:

Firmato digitalmente da: MARTA COLONNA  
Data: 14/12/2022 17:05:23

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]*

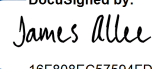
Name: Mixpanel, Inc.

Address: One Front Street, 28th Floor, San Francisco, CA 94111

Contact person's name, position and contact details: General Counsel, compliance@mixpanel.com

Activities relevant to the data transferred under these Clauses: provision of Application Services by importer to exporter.

Signature and date:

DocuSigned by:  
  
16F808EC57594FD...  
12/1/2022

Role (controller/processor): Processor

#### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

End Users of the exporter

*Categories of personal data transferred*

Categories of personal data include navigation, diagnostic and usage data related to the exporter's services and products, unique identifiers and other Personal Data that the exporter may submit through the Application Services the extent of which is determined and controlled by the exporter in its sole discretion as applicable to fulfil the purpose

*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.*

Some diagnostic events related to sensitive data (e.g. diagnostic data related to EU Covid Certificates) may be processed for public interest purposes and for a limited period of time, as applicable in relation to events collected and exclusively determined by the exporter in its sole discretion for its institutional tasks.

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

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter.

*Nature of the processing*

Provision of the activities identified in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter. Processing shall include collection, storage, consultation, organisation, erasure, as the case may be.

*Purpose(s) of the data transfer and further processing*

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter.

*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 Application Services under the Agreement or on exporter's request (ii) for different retention periods for specific datasets are custom set by the exporter, taking into account the nature and purpose of the processing, and are implemented by the importer upon request.

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter. Duration is limited to execution of the activities defined therein.

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

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter. Duration is limited to execution of the activities defined therein.

## **C. COMPETENT SUPERVISORY AUTHORITY**

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 who data are being transferred pursuant to these Clauses are located.

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

<b>TECHNICAL AND ORGANISATIONAL MEASURES</b>	
<b>Measures pseudonymising and/or encrypting personal data</b>	Mixpanel maintains Customer Content encrypted in transit with TLS and at rest with AES 256-bit encryption.
<b>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</b>	The infrastructure for the Application Services spans multiple fault-independent availability zones in geographic regions physically separated from one another; a variety of tools and processes are in place to maintain high availability and resiliency.
<b>Measures ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</b>	Backups of the Customer Content are performed on a regular schedule and recovery testing is periodically conducted. Customer Content is encrypted in transit with TLS and at rest with AES 256 bit encryption.
<b>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</b>	<p>Mixpanel maintains an enterprise-wide security program that includes administrative, organizational, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Customer Content.</p> <p>Mixpanel conducts periodic reviews of its security program through various internal and independent third-party auditing services.</p>
<b>Measures for user and identification authorisation</b>	Mixpanel enforces password and multi-factor authentication requirements. Access rights are promptly removed with personnel termination. Mixpanel operates under the principle of least privilege which ensures that only those with a business need to access a system or data are authorized and utilizes role-based access controls (RBAC) to provision and control access.
<b>Measures for the protection of data during transmission</b>	Mixpanel maintains Customer Content encrypted in transit with TLS.
<b>Measures for the protection of data during storage</b>	Mixpanel maintains Customer Content encrypted with AES-256 bit encryption.
<b>Measures for ensuring physical security of locations at which personal data are processed</b>	Customer Content is stored in the Google Cloud. . Google Cloud data centers physical security features a layered security model. Google Cloud data centers are monitored twenty-four (24) hours a day, seven (7) days a week via



	<p>video surveillance and intrusion detection systems. Access to Google Cloud data centers floor is secured by multi-factor access control including security badges and biometrics. Further information on Google Cloud security program can be found on Google Cloud Compliance Center at <a href="https://cloud.google.com/security/compliance/">https://cloud.google.com/security/compliance/</a>.</p>
<b>Measures for ensuring events logging</b>	<p>Mixpanel maintains application and infrastructure event logs. Events logs are managed centrally and contextually by the security team.</p>
<b>Measures for ensuring system configuration, including default configuration</b>	<p>Mixpanel maintains a change management policy with approval processes applicable to pre-production. Hardened security configuration and vulnerability fixes are used in the production environment. Pre-production and production environments are segregated.</p> <p>Mixpanel leverage tools to minimize security exposure including essential built-in security features such as minimal read-only root file system, file system integrity check, locked-down firewall, and audit logging.</p>
<b>Measures for internal IT and IT security governance and management</b>	<p>The security program at Mixpanel includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Content taking into account the nature of the services provided by Mixpanel and data protection laws and regulations applicable to Mixpanel in its performance of its services. Mixpanel maintains information security and privacy policies considering these aspects. These policies are approved by management, regularly reviewed, and made available to all employees.</p>
<b>Measures for certification/assurance of processes and products</b>	<p>Mixpanel carries various third-party audits and maintains an active SOC 2 Type II certification and performs annual penetration testing.</p>
<b>Measures for ensuring data minimisation</b>	<p>Mixpanel customers determine the data sent to the Application Services and control the amount of data processed for minimization purposes. Customers may delete, modify or retrieve their Customer Content directly through the Application Services. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<b>Measures for ensuring data quality</b>	<p>Mixpanel customers determine the data sent to the Application Services. Customers may delete, modify or retrieve their Customer Content directly through the Application Services. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<b>Measures for ensuring limited data retention</b>	<p>Customers may delete at any time their Customer Content directly through the Application Services. Additionally, Mixpanel deleted the Customer Content at Customer's</p>



request in accordance with the data processing addendum in place with its customers. More on the tools available to customers is available here: <https://developer.mixpanel.com/docs/privacy-security#manage-personal-data>.

**Measures for ensuring accountability**

Mixpanel employs multiple controls to ensure high visibility and enforcement of change management policies to ensure accountability., including comprehensive system logs, code reviews, infrastructure as code, and filtering requests through a centralized ticketing solution.

**Measures for allowing data portability and ensuring erasure**

Customers may delete at any time their Customer Content directly through the Application Services. Additionally, Mixpanel deleted the Customer Content at Customer's request in accordance with the data protection addendum in place with its customers. More on the tools available to customers is available here: <https://developer.mixpanel.com/docs/privacy-security#manage-personal-data>.

**For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

Mixpanel subprocessors pursuant to the data processing addendum with its customers entered into written agreements with Mixpanel requiring that them to abide by terms consistent with the requirements of processing addendum with its customers.

**ANNEX III****LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors:

Sub-Processor	Purpose	Location
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

## DPA Annex 3

### Standard Contractual Clauses (Processor to Processors)

#### 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) (1) 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), (e), (f), and (g);
  - (iii) Clause 9(a), (d) and (f);
  - (iv) Clause 12(a), (d), and (f)
  - (v) Clause 13;



- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e); and
- (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 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.

#### **8.1 Instructions**

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) 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.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.



- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

## **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 controller, as communicated to the data importer by the data exporter, or 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 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, and, where appropriate and feasible, the controller, 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 controller so that the latter may in turn 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 controller, as communicated to the data importer by 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 or the controller 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 controller.

- (c) The data importer shall make available all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) Where an audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (e) 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.
- (f) 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 controller'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 thirty (30) days in advance, thereby giving the data controller 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 controller 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 controller), 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. (8) 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 or controller'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 and, where appropriate, the controller, 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 controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 of the controller, as communicated by 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; or

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; or

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 (12);
  - (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). The data exporter shall forward the notification to the controller.
- (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 [for Module Three: the controller or] 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.

The data exporter shall forward the notification to the controller.

- (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.). The data exporter shall forward the information to the controller.
- (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).
- (f) 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. The data exporter shall make the assessment available to the controller.
- (b) 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:



- (iii) 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;
- (iv) the data importer is in substantial or persistent breach of these Clauses; or
- (v) 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 and the controller 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.

- (i) 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.
- (d) 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 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 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

##### Data exporter(s):

Name: PagoPA S.p.A.

Address: Piazza Colonna 370, CAP 00187, Roma, Italy (seat) - Via Sardegna 38, CAP 00187 (HQ)

Contact person's name, position and contact details: Marta Colonna, DPO, dpo@pagopa.it

Activities relevant to the data transferred under these Clauses: provision of Application Services by importer to exporter.

Signature and date:

Firmato digitalmente da: MARTA COLONNA  
Data: 14/12/2022 17:05:26

Role (controller/processor): Controller

##### Data importer(s):

Name: Mixpanel, Inc.

Address: One Front Street, 28th Floor, San Francisco, CA 94111

Contact person's name, position and contact details: General Counsel, compliance@mixpanel.com

Activities relevant to the data transferred under these Clauses: provision of Application Services by importer to exporter.

Signature and date:

DocuSigned by:  
*James Allee*  
16F808EC57594FD...  
12/1/2022

Role (controller/processor): Processor

#### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

End Users of the exporter

*Categories of personal data transferred*

Categories of personal data include navigation, diagnostic and usage data related to the exporter's services and products, unique identifiers and other Personal Data that the exporter may submit through the Application Services the extent of which is determined and controlled by the exporter in its sole discretion as applicable to fulfil the purpose

*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.

Some diagnostic events related to sensitive data (e.g. diagnostic data related to EU Covid Certificates) may be processed for public interest purposes and for a limited period of time, as applicable in relation to events collected and exclusively determined by the exporter in its sole discretion for its institutional tasks.

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

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter.

*Nature of the processing*

Provision of the activities identified in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter. Processing shall include collection, storage, consultation, organisation, erasure, as the case may be.

*Purpose(s) of the data transfer and further processing*

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter.

*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 Application Services under the Agreement or on exporter's request (ii) for different retention periods for specific datasets are custom set by the exporter, taking into account the nature and purpose of the processing, and are implemented by the importer upon request.

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

As determined in the Data Residency Certification executed by the importer on July 19, 2021, as it may be modified from time to time in writing upon agreement between the importer and the exporter. Duration is limited to execution of the activities defined therein.

## **C. COMPETENT SUPERVISORY AUTHORITY**

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 who data are being transferred pursuant to these Clauses are located.

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

<b>TECHNICAL AND ORGANISATIONAL MEASURES</b>	
<b>Measures pseudonymising and/or encrypting personal data</b>	Mixpanel maintains Customer Content encrypted in transit with TLS and at rest with AES 256-bit encryption.
<b>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</b>	The infrastructure for the Application Services spans multiple fault-independent availability zones in geographic regions physically separated from one another; a variety of tools and processes are in place to maintain high availability and resiliency.
<b>Measures ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</b>	Backups of the Customer Content are performed on a regular schedule and recovery testing is periodically conducted. Customer Content is encrypted in transit with TLS and at rest with AES 256 bit encryption.
<b>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</b>	<p>Mixpanel maintains an enterprise-wide security program that includes administrative, organizational, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Customer Content.</p> <p>Mixpanel conducts periodic reviews of its security program through various internal and independent third-party auditing services.</p>
<b>Measures for user and identification authorisation</b>	Mixpanel enforces password and multi-factor authentication requirements. Access rights are promptly removed with personnel termination. Mixpanel operates under the principle of least privilege which ensures that only those with a business need to access a system or data are authorized and utilizes role-based access controls (RBAC) to provision and control access.
<b>Measures for the protection of data during transmission</b>	Mixpanel maintains Customer Content encrypted in transit with TLS.
<b>Measures for the protection of data during storage</b>	Mixpanel maintains Customer Content encrypted with AES-256 bit encryption.
<b>Measures for ensuring physical security of locations at which personal data are processed</b>	Customer Content is stored in the Google Cloud. . Google Cloud data centers physical security features a layered security model. Google Cloud data centers are monitored twenty-four (24) hours a day, seven (7) days a week via



	<p>video surveillance and intrusion detection systems. Access to Google Cloud data centers floor is secured by multi-factor access control including security badges and biometrics. Further information on Google Cloud security program can be found on Google Cloud Compliance Center at <a href="https://cloud.google.com/security/compliance/">https://cloud.google.com/security/compliance/</a>.</p>
<b>Measures for ensuring events logging</b>	<p>Mixpanel maintains application and infrastructure event logs. Events logs are managed centrally and contextually by the security team.</p>
<b>Measures for ensuring system configuration, including default configuration</b>	<p>Mixpanel maintains a change management policy with approval processes applicable to pre-production. Hardened security configuration and vulnerability fixes are used in the production environment. Pre-production and production environments are segregated.</p> <p>Mixpanel leverage tools to minimize security exposure including essential built-in security features such as minimal read-only root file system, file system integrity check, locked-down firewall, and audit logging.</p>
<b>Measures for internal IT and IT security governance and management</b>	<p>The security program at Mixpanel includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Content taking into account the nature of the services provided by Mixpanel and data protection laws and regulations applicable to Mixpanel in its performance of its services. Mixpanel maintains information security and privacy policies considering these aspects. These policies are approved by management, regularly reviewed, and made available to all employees.</p>
<b>Measures for certification/assurance of processes and products</b>	<p>Mixpanel carries various third-party audits and maintains an active SOC 2 Type II certification and performs annual penetration testing.</p>
<b>Measures for ensuring data minimisation</b>	<p>Mixpanel customers determine the data sent to the Application Services and control the amount of data processed for minimization purposes. Customers may delete, modify or retrieve their Customer Content directly through the Application Services. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<b>Measures for ensuring data quality</b>	<p>Mixpanel customers determine the data sent to the Application Services. Customers may delete, modify or retrieve their Customer Content directly through the Application Services. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<b>Measures for ensuring limited data retention</b>	<p>Customers may delete at any time their Customer Content directly through the Application Services. Additionally, Mixpanel deleted the Customer Content at Customer's</p>



	<p>request in accordance with the data processing addendum in place with its customers. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<p><b>Measures for ensuring accountability</b></p>	<p>Mixpanel employs multiple controls to ensure high visibility and enforcement of change management policies to ensure accountability., including comprehensive system logs, code reviews, infrastructure as code, and filtering requests through a centralized ticketing solution.</p>
<p><b>Measures for allowing data portability and ensuring erasure</b></p>	<p>Customers may delete at any time their Customer Content directly through the Application Services. Additionally, Mixpanel deleted the Customer Content at Customer's request in accordance with the data protection addendum in place with its customers. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<p><b>For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter</b></p>	<p>Mixpanel subprocessors pursuant to the data processing addendum with its customers entered into written agreements with Mixpanel requiring that them to abide by terms consistent with the requirements of processing addendum with its customers.</p>



**ANNEX III**

**LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors:

Sub-Processor	Purpose	Location
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

**TECHNICAL AND ORGANISATIONAL MEASURES**

<p><b>Measures pseudonymising and/or encrypting personal data</b></p>	<p>Mixpanel maintains Customer Content encrypted in transit with TLS and at rest with AES 256-bit encryption.</p>
<p><b>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</b></p>	<p>The infrastructure for the Application Services spans multiple fault-independent availability zones in geographic regions physically separated from one another; a variety of tools and processes are in place to maintain high availability and resiliency.</p>
<p><b>Measures ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</b></p>	<p>Backups of the Customer Content are performed on a regular schedule and recovery testing is periodically conducted. Customer Content is encrypted in transit with TLS and at rest with AES 256 bit encryption.</p>
<p><b>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</b></p>	<p>Mixpanel maintains an enterprise-wide security program that includes administrative, organizational, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Customer Content.</p> <p>Mixpanel conducts periodic reviews of its security program through various internal and independent third-party auditing services.</p>
<p><b>Measures for user and identification and authorisation</b></p>	<p>Mixpanel enforces password and multi-factor authentication requirements. Access rights are promptly removed with personnel termination. Mixpanel operates under the principle of least privilege which ensures that only those with a business need to access a system or data are authorized and utilizes role-based access controls (RBAC) to provision and control access.</p>
<p><b>Measures for the protection of data during transmission</b></p>	<p>Mixpanel maintains Customer Content encrypted in transit with TLS.</p>
<p><b>Measures for the protection of data during storage</b></p>	<p>Mixpanel maintains Customer Content encrypted with AES-256 bit encryption.</p>
<p><b>Measures for ensuring physical security of locations at which personal data are processed</b></p>	<p>Customer Content is stored in the Google Cloud. . Google Cloud data centers physical security features a layered security model. Google Cloud data centers are monitored twenty-four (24) hours a day, seven (7) days a week via video surveillance and intrusion detection systems. Access to Google Cloud data centers floor is secured by multi-factor access control including security badges and</p>



	<p>biometrics. Further information on Google Cloud security program can be found on Google Cloud Compliance Center at <a href="https://cloud.google.com/security/compliance/">https://cloud.google.com/security/compliance/</a>.</p>
<b>Measures for ensuring events logging</b>	<p>Mixpanel maintains application and infrastructure event logs. Events logs are managed centrally and contextually by the security team.</p>
<b>Measures for ensuring system configuration, including default configuration</b>	<p>Mixpanel maintains a change management policy with approval processes applicable to pre-production. Hardened security configuration and vulnerability fixes are used in the production environment. Pre-production and production environments are segregated.</p> <p>Mixpanel leverage tools to minimize security exposure including essential built-in security features such as minimal read-only root file system, file system integrity check, locked-down firewall, and audit logging.</p>
<b>Measures for internal IT and IT security governance and management</b>	<p>The security program at Mixpanel includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Content taking into account the nature of the services provided by Mixpanel and data protection laws and regulations applicable to Mixpanel in its performance of its services. Mixpanel maintains information security and privacy policies considering these aspects. These policies are approved by management, regularly reviewed, and made available to all employees.</p>
<b>Measures for certification/assurance of processes and products</b>	<p>Mixpanel carries various third-party audits and maintains an active SOC 2 Type II certification and performs annual penetration testing.</p>
<b>Measures for ensuring data minimisation</b>	<p>Mixpanel customers determine the data sent to the Application Services and control the amount of data processed for minimization purposes. Customers may delete, modify or retrieve their Customer Content directly through the Application Services. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<b>Measures for ensuring data quality</b>	<p>Mixpanel customers determine the data sent to the Application Services. Customers may delete, modify or retrieve their Customer Content directly through the Application Services. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<b>Measures for ensuring limited data retention</b>	<p>Customers may delete at any time their Customer Content directly through the Application Services. Additionally, Mixpanel deletes the Customer Content at Customer's request (which may include Customer's custom retention requirements) in accordance with the data processing</p>





	<p>addendum in place with its customers. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<p><b>Measures for ensuring accountability</b></p>	<p>Mixpanel employs multiple controls to ensure high visibility and enforcement of change management policies to ensure accountability., including comprehensive system logs, code reviews, infrastructure as code, and filtering requests through a centralized ticketing solution.</p>
<p><b>Measures for allowing data portability and ensuring erasure</b></p>	<p>Customers may delete at any time their Customer Content directly through the Application Services. Additionally, Mixpanel deletes the Customer Content at Customer's request in accordance with the data protection addendum in place with its customers. More on the tools available to customers is available here: <a href="https://developer.mixpanel.com/docs/privacy-security#manage-personal-data">https://developer.mixpanel.com/docs/privacy-security#manage-personal-data</a>.</p>
<p><b>For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter</b></p>	<p>Mixpanel subprocessors pursuant to the data processing addendum with its customers entered into written agreements with Mixpanel requiring that them to abide by terms consistent with the requirements of processing addendum with its customers.</p>



## DPA Annex 5

### LIST OF SUB-PROCESSORS

**Sub-processors.** For the purposes of Clauses 8.8 and 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 said purposes:

(i) A list of approved sub-processors is available to the Data Exporter under this Annex. Customer undertakes not to publish or otherwise disclose such list to the public except as necessary to comply with an order or subpoena of any authority (including any competent supervisory authority) or a court of competent jurisdiction, or as reasonably necessary to comply with any applicable law or regulation. Any request for disclosure of such list, received by Customer, shall be notified or redirected to Mixpanel (by emailing [compliance@mixpanel.com](mailto:compliance@mixpanel.com)) as the case may be, unless Customer is legally prohibited from doing so.

(ii) Prior notification of updates to the list of sub-processors requires Data Exporter to first submit a request for such notifications in writing to Mixpanel by emailing [compliance@mixpanel.com](mailto:compliance@mixpanel.com). Data Importer will then provide Data Exporter with a copy of Data Importer's Subprocessor list within 30 days and send Data Exporter updates to such Subprocessor list (if any) in accordance with the DPA.

(iii) Any such subprocessors will be permitted to process Personal Data only to deliver the services Mixpanel has retained them to provide in the DPA, and they shall be prohibited from using Personal Data for any other purpose.

For the purposes of this DPA, Customer has authorised the use of the following sub-processors:

Sub-Processor	Purpose	Location	Data	Retention
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]



			[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

**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.