mixpanel

AMENDMENT NO. 1 TO GDPR DATA PROCESSING ADDENDUM

This Amendment No. 1 to GDPR Data Processing Addendum (this "Amendment") is effective as of the date of the last signature set forth below (the "Effective Date") by and among Mixpanel, Inc. (the "Company") and PagoPA S.p.A. (the "Customer"). All capitalized terms used in this Amendment but not defined herein shall have the meanings ascribed to them in that certain Mixpanel GDPR Data Processing Addendum signed on March 31, 2020 (the "DPA").

Recitals

The Company and the Customer are parties to the DPA. The Company and the Customer desire to amend the DPA as set forth herein.

Agreement

In consideration of the foregoing recitals and for other consideration, the adequacy and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

1. Amendments.

   a. Section 9 of the Data Processing Terms of the DPA is hereby amended and restated as follows:

      "9 Agrees, where Mixpanel Processes or permits any Subprocessor to Process Personal Data in any country not deemed to provide an adequate level of protection of Personal Data by Data Protection Legislation, to transfer such Personal Data across international borders as follows: (i) for the European Union or the European Economic Area in compliance with the Standard Contractual Clauses which shall be incorporated in full by reference and form an integral part of this DPA, and which are set forth in Annex 2 below, provided that in the event of a conflict between the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall control, (ii) for the United Kingdom, in compliance with the Standard Contractual Clauses, which the Parties agree shall apply to such transfer, and (iii) for Switzerland pursuant to the Swiss-U.S. Privacy Shield provided that Mixpanel maintains its certification under the Swiss-U.S. Privacy Shield;"

   b. The attached Exhibit A is hereby added as Annex III to the DPA.

2. Effect. Except as specifically modified herein, all terms and conditions of the DPA shall continue in full force and effect. In the event of conflict between a provision or provisions of this Amendment and any provision or provisions of the DPA, the provision or provisions of this Amendment shall control.

[*Signatures to follow*]

IN WITNESS WHEREOF, the parties have caused this Amendment to be executed by their respective authorized representatives.

Executed by:

Mixpanel, Inc.	PagoPA S.p.A.
DocuSigned by: Peter Day 6B6C0360902A4FF... Signature	DocuSigned by: Giuseppe Virgone F1AF6FDE131F4F4... Signature
Print Name: Peter Day	Print Name: Giuseppe Virgone
Print Title: Head of Global Privacy	Print Title: CEO
Date: 10/16/2020	Date: 10/14/2020

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 46(2) of Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: PagoPA S.p.A.

Address: Piazza Colonna 370, CAP 00187, Roma, Italy

e-mail: dpo@pagopa.it

Other information needed to identify the organisation: Company registration number, Tax code and VAT: 15376371009

(the data **exporter**)

And

Name of the data importing organisation: Mixpanel Inc.

Address: One Front Street, 28th Floor, San Francisco, California 94111, United States

e-mail: dpo@mixpanel.com

Other information needed to identify the organisation:

…

(the data **importer**)

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 and regulated by the Master Services Agreement and the Data Processing Addendum entered into between the data importer and the data exporter on 28 February 2020 and subsequently integrated on 27 July 2020.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in 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, and repealing Directive 95/46/EC ;

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 45 of Regulation (EU) 2016/679 ;

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Regulation (EU) 679/2016 ;

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Italy

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses . Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Italy

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

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

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Obligations related to data transfer under foreign law

1. The data importer will provide information to the data exporter prior to responding to or answering any binding obligation provided under foreign law to communicate data of the data exporter to a law enforcement or a government agency, and of any related prohibition preventing it from informing the data exporter.

2. The data importer will provide prior notice to the data exporter on any request it receives to communicate data of the data exporter to a law enforcement or government agency. The data importer will use its best efforts to obtain the right to waive a prohibition preventing it from informing the data exporter of a legally binding request for disclosure of personal data.

3. The data importer represents and warrants that it will adopt internal procedures to provide consistent and accountable means for responding to such requests and, at request, will provide evidence thereof.

4 The data importer will ensure that any disclosures of personal data by the data importer are reasonable, proportionate and have an appropriate legal basis.

Clause 14

Amendment to the Data Processing Addendum

1.The Data Processing Addendum is amended as it follows. Sec. 9 is amended and restated as it follows :

> “ Mixpanel may transfer data outside the EEA on the basis of valid standard contractual clauses agreed with Customer and it will make sure to enter into adequate standard contractual clauses with its subprocessors, for the duration of this Data Processing Addendum”

On behalf of the data exporter:

Name (written out in full): Giuseppe Virgone

Position: Amministratore Unico

Address:, Piazza Colonna 370, CAP 00187, Roma, Italy

Signature: DocuSigned by: Giuseppe Virgone F1AF6FDE131F4F4...

On behalf of the data importer:

Name (written out in full): Peter Day

Position: Head of Global Privacy

Address: One Front Street, 28th Floor, San Francisco, California 94111, United States

Signature DocuSigned by: Peter Day 6B6C0360902A4FF...

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is:

PagoPA S.p.A.

Data importer

The data importer is :

Mixpanel, Inc

Data subjects

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

end users of the data exporter

Categories of data

The personal data transferred concern the following categories of data (please specify):

Event data, Navigation data, device data, end users identifiers, as better identified and listed in the Data Processing Addendum

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The provision of Application Services by Mixpanel to Customer.

DATA EXPORTER

Name: PagoPA S.p.A.

Authorised Signature …

DocuSigned by:
Giuseppe Virgone
F1AF6FDE131F4F4...

DATA IMPORTER

Name: Mixpanel Inc.

Authorised Signature …

DocuSigned by:
Peter Day
6B6C0360902A4FF...

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The data exporter has the ability to configure its products to send the data directly to the data importer's proprietary data store for instant analysis. The data importer is fully HTTPS capable for all data transmission. Once stored, raw data are only accessible via API using private and secret key authentication. Data importer's infrastructure is implemented on the solution of Cloud Service Provider Google (GCP - Google Cloud Platform). Stored data is:

- encrypted at rest;
- logically separated from any other client's data;
- redundant (in production);
- backed up at a geographically separate location.

The data importer only processes those actions that have been programmatically defined in the source code. When a user visits a website or application with the data importer's service instrumented, the details of their interactions are captured and sent to the data importer through API calls over HTTPS/HTTP.

The data exporter's users access the data on importer's servers through a web interface; for this access two-factor authentication and single sign-on features are available. Other ways of accessing consist in the use of a number of APIs that are authenticated through key/secret credential combinations. Citizen access is not recorded on audit trail at the individual user level.

DATA PROCESSED

The data importer processes data only from the data exporter's app (where library or SDK is installed), or from Internet connected devices that initiate requests to the data importer's REST API, as programmatically defined by the data exporter, within the application source code.

The data importer relies upon third parties for Internet protocol (IP) address intelligence, for databases of information that can help analyze data, but do not send data exporter's data to them. IP addresses are not stored unless the data exporter specifically enables it in the course of the data collection service configuration.

All data processing activities are logically isolated between customers. There is no way to correlate between users of two different customers, even if they are the same person.

PRIVACY & CONFIDENTIALITY

The data importer takes all the steps needed to protect personal information in order to prevent loss, misuse, and unauthorized access, disclosure, alteration and destruction.

DATA CENTER SECURITY & LOCATION

The data importer servers that persistently store customer data are hosted by Google Cloud Platform. GCP's data center is SOC 1, SOC 2 and SOC 3 compliant. Additionally, Google logically isolates each customer's Cloud Platform data from that of other customers and users.

GLOBAL DISTRIBUTION

The data importer has been architected to receive data from many regions around the globe.

The data importer maintains endpoint clusters and uses dynamic DNS to route requests to the endpoint that is geographically closest to the client. These endpoints queue the incoming data and perform initial validation and sorting.

DATA CENTER FEATURES

ALL GCP DATA CENTER FACILITIES INCLUDE

- Strict access security:
    - custom-designed electronic access cards;
    - alarms;
    - vehicle access barriers;
    - perimeter fencing;
    - metal detectors;
    - biometrics;
    - data center floor features laser beam intrusion detection.
- Monitoring:
    - 24/7 high-resolution interior and exterior cameras that can detect and track intruders;
    - access logs;
    - activity records;
    - camera footage is available in case of incident.
- Personnel:
    - patrolled by experienced security guards;
    - rigorous background checks and training.
- Power availability:
    - redundant power systems;

  - environmental controls;
  - diesel engine backup generators - enough emergency electrical power to run at full capacity;
  - cooling systems;
  - fire detection and suppression equipment.

DATA PROTECTION

All data sent over HTTPS to and from the data importer uses 256-bit encryption in transit. Data flows from the API clusters to the production data stores via GCP’s backbone network infrastructure. Data is encrypted at rest, and it is stored in a proprietary analytics database format (i.e. not an off-the-shelf database). This database infrastructure was designed for high-speed queries with security in mind. Additionally, Google logically isolates the data importer’s Cloud Platform data from that of other customers and users.

Each data importer’s project is logically separated from all other projects, so although the data is stored on shared hardware, the database architecture prevents data in one project from leaking into other projects. The data importer's information assets are systematically identified and documented. An asset repository is in place recording the information that allows to implement proper security measures on the basis of their criticality (determined through the classification of processed information).

APPLICATION SECURITY

The data importer maintains a robust and comprehensive application security program. Security is an integral part of its entire development process:

- At design time, through security design reviews and threat modeling.
- At implementation time, with comprehensive security development training, secure code review guidelines, and static analysis tools to identify vulnerable code.
- At deployment time, with strict manual and automated code review requirements and automated deployment processes.
- In operation, with ongoing automated vulnerability scans, and monitoring controls to identify denial-of-service attacks.

Application monitoring controls are in place to identify denial- of-service attacks.

Additionally, an independent 3rd party performs application-level penetration tests annually. All issues emerging from this kind of tests are addressed, prioritizing critical ones, through the data importer change management process in order to resolve any exploitable vulnerability that is found during the test.

SECURITY POLICY

The data importer maintains compliance with the most demanding, security conscious enterprises.

Security Policies that cover the following topics are maintained and updated annually:

- Employee Security Awareness Training;
- Information Resource Management;
- Information Classification;
- Information Security Compliance;
- Access Controls;
- Technical Security;
- Encryption;
- Firewall Security;
- Administrative Safeguards;
- Vendor Security;
- Security Monitoring;
- Information Access;
- Secure Workspace;
- Physical Security.

AUDITS

The data importer undergoes annual security assessments by an independent, third party security firm.

These assessments ensure that the data importer is performing all of the necessary measures to protect production systems and ensure the integrity of the data exporter’s data.

SECURITY CONFIGURATION

CONFIGURATION AND CHANGE CONTROL MANAGEMENT

Security risk analysis is conducted when implementing new components in production or development environments. Every change to application code is thoroughly reviewed for functional and security issues. A standard base image is used for all new systems, which are deployed by GCP. Machines are then customized to fit their role. These procedures are documented and audited.

DMZ

Following industry standard best practices, the data importer implements a “Demilitarized Zone” (DMZ). The DMZ is used to limit inbound and outbound traffic only to protocols that are necessary for the secure data environment. Firewalls have been implemented at each Internet connection and between the DMZ and internal network zone.

VULNERABILITY SCANS & AUDITS

The data importer runs automated network vulnerability scans on an ongoing basis. Third-party penetration tests are performed annually. Penetration tests include testing against the network perimeter from the Internet. High-risk vulnerabilities are resolved within 90 days of discovery.

UPDATES & ANTI-VIRUS SOFTWARE

The data importer uses Linux for all production systems; its strategy to protect these Linux servers is to focus on making the production systems immutable and frequently recycle them. This prevents malware from gaining a persistent foothold, and ensures that there is a minimal window in which malware could stay memory-resident.

Whenever a new vulnerability is discovered, software is updated within a month.

MONITORING

The data importer employs an in-house Security Information and Event Management platform, which provides 24x7x365 monitoring and alerting for security incidents in networks and systems.

The SIEM collects information from the corporate infrastructure, from the cloud hosting provider, and from the production services, providing a comprehensive view of security-related activities.

Google, the cloud hosting provider, adds further layers of monitoring, inspecting internal traffic at many points across their global network for suspicious behavior, such as the presence of traffic that might indicate botnet connections. Their network analysis is supplemented by automated analysis of system and network logs to identify unusual behavior, such as attempted access of customer data.

ACCESS CONTROL MEASURES

Access is granted to production servers only as required and is provisioned on an as-needed basis.

The data importer systems are equipped with technical and administrative measures for identifying its users, the user's rights to the systems, and the recording of:

- all accesses of the data importer’s users[1];
- users’ activities.

All records contain at least this information:

[1] System administrators, devops user or whoever may access the data exporter’s conferred PIIs

- user's identity;
- timestamps of login and logout and other activities;
- a description of the activity;
- source IP.

Registered events (logs) are:

- stored securely and kept in their unchanged condition;
- protected against intrusion / unauthorized access / modification.

Recorded information is stored for at least six months.

INCIDENT RESPONSE

The data importer Incident Response Team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Any and all suspected or confirmed Data Security Incidents must be immediately reported to the Data Protection Officer. The DPO will engage the Incident Response Team and coordinate with management and the Legal Department to determine appropriate actions that will be taken in accordance with this policy to meet the data importer's legal obligations and to prevent or mitigate impact to consumers, employees or The data importer resulting from a Data Security Incident.

Roles and responsibilities of all individuals on the Incident Response Team are well documented in the data importer's Data Security Incident Response Plan.

Any breach impacting PIIs conferred to the data importer by the data exporter will be promptly (within 24h from its formal detection) communicated to the latter representatives in order to allow them to comply with any obligation that should arise from it.

BUSINESS CONTINUITY & DISASTER RECOVERY

The data importer maintains a Disaster Recovery (DR) plan for its service. This plan is regularly updated and tested. All data in the production environment will be frequently snapshotted and stored durably in multiple geographic locations in the US. Backups are maintained for the duration of the customer relationship and for one year after the termination of an agreement unless otherwise specified (by the data exporter) or required by law.

DATA EXPORTER

Name: PagoPA S.p.A.

Authorised Signature …

DocuSigned by:

Giuseppe Virgone

F1AF6FDE131F4F4...

DATA IMPORTER

Name: Mixpanel Inc.

Authorised Signature …

DocuSigned by:

Peter Day

6B6C0360902A4FF...