



ethnio™

DATA PROCESSING ADDENDUM (DPA)

VERSION NO. 1
CREATED TUESDAY,
MAY 15, 2018

ETHNIO, INC.
6121 W SUNSET BLVD
LOS ANGELES, CA 90028
TEL (888) 879-7439
ETHN.IO



INTRODUCTION

Ethnio is dedicated to processing personal data in a secure, fair, and transparent manner. As part of this effort, we process personal data in accordance with the EU's General Data Protection Regulation ("GDPR"), the EU/US Privacy Shield principles ("Privacy Shield"), the laws of the US governing the handling of various types of personal data (including HIPAA), and industry standards, such as PCI.

To better protect individuals' personal data, we are providing these terms to govern Ethnio's and your handling of personal data (the "Data Processing Addendum" or "DPA"). This DPA amends and supplements your Terms and Conditions and requires no further action on your part.

If you do not agree to this DPA, you may discontinue the use of the Ethnio service and cancel your account.

DEFINITIONS

It is important that all parties understand what data and whose data is protected under this DPA. Each party has respective obligations to protect personal; therefore, the following definitions explain the scope of this DPA and the mutual commitments to protect personal data. "Ethnio", "we", "us", or "our" refers to the provider of the Ethnio website and services, (collectively referred to as the "Ethnio Service.").

"**You**" or "**Customer**" refers to the company or organization that signs up to use the Ethnio Service to manage the relationships with your consumers or service users.

"**Party**" refers to Ethnio and/or the customer depending on the context.

"**Personnel**" refers to those individuals who are employed by or are under contract to perform a service on behalf of one of the parties. Personnel may have rights in their personal data



(including business contact information) if they reside in the EU. It is important to be clear about how personnel's rights are protected.

“Data Subjects” refers to those individuals residing in the EU who are consumers or users of a Ethnio Customer's goods or services (also “consumers”), as well as any personnel who reside in the EU.

“Personal Data” is given the same meaning as in the GDPR which we summarize here as: any data relating directly or indirectly to an identifiable data subject. Personal data does not include any data that is anonymized, aggregated, de-identified and/or compiled on a generic basis and which does not name or identify a specific individual, directly or indirectly.

“Processing” is given the same meaning as in the GDPR, which we summarize as including: collecting, recording, using, storing, amending, adapting, disclosing, transferring or transmitting, structuring, using, combining, deleting or destroying, personal data (“Process” and “Processed” shall have similar meanings).

“Controller” is given the same meaning as in the GDPR, which we summarize as the party that determines the purposes and means of the processing of personal data – the customer is the controller with respect to consumer personal data. Each party may be the controller of personal data it processes about the other's personnel.

“Processor” is the party that processes personal data on behalf of the controller – Ethnio is the processor of the personal data we process about your consumers.

“Incident” means: (a) a complaint or a request with respect to the exercise of an individual's rights under the GDPR; (b) an investigation into or seizure of the personal data by government officials, or a specific indication that such an investigation or seizure is imminent; or (c) any breach of the security and/or confidentiality as set out in this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the personal data, or any indication of such breach having taken place or being about to take place.

For the sake of readability, we do not use initial capitalization of defined terms in this DPA. Defined terms are defined terms, irrespective of their format.



UNDERTAKINGS REGARDING PERSONAL DATA

1. Each party agrees that personal data shall be treated as confidential information under this DPA. In addition, each party shall at all times comply with applicable laws relating to data protection in the relevant jurisdiction with respect to each other's personal data.
2. Personal Data shall remain the property of the disclosing party. Ethnio acknowledges that customer is the controller and maintains control over data subject's personal data.
3. Ethnio will process customer's personal data only to the extent strictly necessary for the purpose of providing the services in accordance with the ToS and any further written instructions from the customer that are mutually agreed upon in writing. Ethnio agrees that:
 - 3.1. it will implement and maintain a reasonable and appropriate security program comprising adequate security, technical and organizational measures to protect against unauthorized, unlawful or accidental processing, use, erasure, loss or destruction of, or damage to, customer personal data;
 - 3.2. it will not modify, alter, delete, publish or disclose any customer personal data to any third party, nor allow any third party to process such personal data on Ethnio's behalf unless the third party is bound to similar confidentiality and data handling provisions;
 - 3.3. only its personnel who "need-to-know" will be given access to customer personal data to the extent necessary to perform its obligations under the ToS. It shall provide adequate training to its staff and ensure that they comply with the obligations in this DPA; and
 - 3.4. it will only process customer personal data to the extent necessary to perform its obligations under the ToS, upon written instructions of the customer (only as mutually agreed upon), and in accordance with applicable laws.
4. Upon termination of your account Ethnio will delete, destroy, or anonymize the personal data in accordance with our standard backup and retention policy per the ToS, normally, no later than 60 days, unless we have terminated your account for violation of the ToS in which case Ethnio reserves the right to retain personal data.
5. Ethnio is certified under the EU/US Privacy Shield Framework and, therefore, customer may transfer personal data from the EU to Ethnio, as this transfer mechanism is deemed to be adequate for the purposes of GDPR. Ethnio shall not transfer any



customer personal data outside of the US or to other locations not deemed to be “adequate” under EU law without providing reasonable notice under the ToS to the customer.

6. The parties acknowledge that customer may from time to time be in possession of personal data relating to Ethnio’s personnel. Ethnio warrants that it has provided all necessary notifications and obtained all necessary consents, authorizations, approvals and/or agreements as required under any applicable law in order to enable: (i) the disclosure of Ethnio’s personal data to customer; and (ii) further processing of such Ethnio personal data by customer.

CUSTOMER UNDERTAKINGS AND ETHNIO’S ASSISTANCE

1. Customer warrants that it has all necessary rights to provide to Ethnio the personal data for processing in connection with the provision of the Ethnio Services.
2. To the extent required by applicable law, customer is responsible for ensuring that any data subject consents that may be necessary to this processing are obtained, and for ensuring that a record of such consents is maintained, including any consent to use personal data that is obtained from third parties. Should such consent be revoked by a data subject, customer is responsible for communicating the fact of such revocation to Ethnio, and Ethnio remains responsible for implementing any customer instruction with respect to the further processing of that personal data, or, as may be in accordance with any of Ethnio’s legal obligations.
3. Customer understands, as a controller, that it is responsible (as between customer and Ethnio) for:
 - 3.1. determining the lawfulness of any processing, performing any required data protection impact assessments, and accounting to regulators and individuals, as may be needed;
 - 3.2. making reasonable efforts to verify parental consent when data is collected on a data subject under 16 years of age;



- 3.3. providing relevant privacy notices to data subjects as may be required in your jurisdiction, including notice of their rights and provide the mechanisms for individuals to exercise those rights;
 - 3.4. responding to requests from individuals about their data and the processing of the same, including requests to have personal data altered, corrected, or erased, and providing copies of the actual data processed;
 - 3.5. implementing your own appropriate technical and organizational measures to ensure and demonstrate processing in accord with this DPA;
 - 3.6. notifying individuals and any relevant regulators or authorities of any incident as may be required by law in your jurisdiction.
4. Ethnio shall assist the customer by implementing appropriate technical and organizational measures, insofar as this is reasonably and commercially possible (in Ethnio's sole determination and discretion), in fulfilling customer's obligations to respond to individuals' requests to exercise rights under the GDPR.
 5. Ethnio shall make available to the customer information reasonably necessary to demonstrate compliance with Ethnio's obligations under this DPA. At a minimum, upon written request, Ethnio will produce to Company a copy of any third-party audit reports concerning the adequacy of Ethnio's technical security measures. Company does not have any independent right to audit Ethnio's technical and/or organizational measures.

INCIDENT MANAGEMENT

1. When either party becomes aware of an incident that impacts the processing of personal data, it shall promptly notify the other about the incident and shall reasonably cooperate in order to enable the other party to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.
2. Both parties shall at all times have in place written procedures which enable them to promptly respond to the other about an incident. Where the incident is reasonably likely to require a data breach notification under applicable laws, the party responsible for the



incident shall notify the other no later than 24 hours of having become aware of such an incident.

3. Any notifications made under this section shall be made to info@ethn.io (when made to Ethnio) and to our point of contact with you (when made to the customer), and shall contain:(i) a description of the nature of the incident, including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of records concerned; (ii) the name and contact details of the point of contact where more information can be obtained; (iii) a description of the likely consequences of the incident; and (iv) a description of the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

LIABILITY AND INDEMNITY

1. Each party indemnifies the other and holds them harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the indemnified party and arising directly or indirectly out of or in connection with a breach of this DPA.

DURATION AND TERMINATION

1. This DPA shall come into effect on May 25, 2018 and shall continue until it is changed or terminated in accordance with the ToS.
2. Termination or expiration of this DPA shall not discharge the parties from the confidentiality obligations herein.



SIGNATURE PAGE

IN WITNESS WHEREOF, the authorized representatives of the parties have executed this Agreement.

Ethnio Signature

Date

May 15, 2018

Job Title

CEO

Organization

Ethnio, Inc.

Customer Signature

Date

Job Title

Organization
