

TURNT0 NETWORKS, INC.

DATA PROCESSING ADDENDUM

Effective Date: _____

This Data Processing Addendum (this "**DPA**") is made as of the Effective Date by and between TurnTo Networks, Inc., a corporation organized and existing under the laws of the State of Delaware, U.S.A. ("**TurnTo**"), and the entity or person set forth on the signature page hereto ("**Customer**"), pursuant to the Agreement (as defined below). TurnTo and Customer are sometimes referred to herein individually as a "**party**" or together as the "**parties**".

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data is processed by TurnTo under the Agreement.

1. Definitions

1.1 For the purposes of this DPA, the following terms shall have their respective meanings set forth below and other capitalized terms used but not defined in this DPA have the same meanings as set forth in the Agreement:

- (a) "**Agreement**" means the TurnTo System Terms and Conditions or Master SaaS Agreement, as applicable, between the parties, in each case providing for the provision by TurnTo to Customer of the services described therein.
- (b) "**EEA**" means the European Economic Area (including the United Kingdom).
- (c) "**EU Data Protection Legislation**" means (i) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**Directive**"), including any applicable national implementations of it; and (ii) on and after May 25, 2018, Regulation 2016/679 of the European Parliament and of the Council 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data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**") (as amended, replaced or superseded).
- (d) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- (e) "**Processor**" means an entity which processes Personal Data on behalf of the Controller.
- (f) "**Personal Data**" means any information relating to an identified or identifiable natural person.
- (g) "**Privacy Shield**" means the EU-U.S. self-certification program operated by the U.S. Department of Commerce.
- (h) "**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of July 12, 2016 (as may be amended, superseded or replaced).
- (i) "**Security Incident**" means accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

- (j) **"Sensitive Data"** means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof), (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; (f) date of birth; (g) criminal history; (h) mother's maiden name; and (i) any other information that falls within the definition of "special categories of data" under EU Data Protection Legislation or any other applicable law relating to privacy and data protection.

2. Relationship with Agreement

- 2.1 Except as amended by this DPA, the Agreement will remain in full force and effect.
- 2.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.
- 2.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

3. Applicability of this DPA

- 3.1 Part A (being Sections 4 to 6 as well as Annexes A and B of this DPA), shall apply to the processing of Personal Data under the Agreement from the Effective Date above.
- 3.2 Part B (being Sections 7 to 11 as well as Annex C of this DPA) shall apply to the processing of Personal Data by TurnTo falling within the scope of the GDPR from and including May 25, 2018.
- 3.3 With respect to the processing of Personal Data falling within the scope of Part B:
- (a) the terms of Part B shall apply in addition to, and not in substitution of, the terms in Part A; and
 - (b) to the extent there is any conflict between the provisions in Part A and Part B, the provisions in Part B shall take priority from and including May 25, 2018.
- 3.4 Notwithstanding anything in this DPA, TurnTo will have the right to collect, extract, compile, synthesize and analyze non-personally identifiable data or information resulting from Customer's use or operation of the Services ("**Service Data**") including, by way of example and without limitation, information relating to volumes, frequencies, patterns, or any other information regarding the use of the System by Customer or its end users. To the extent any Service Data is collected or generated by TurnTo, such data will be solely owned by TurnTo and may be used by TurnTo for any lawful business purpose without a duty of accounting to Customer or its recipients, provided that such data is used only in an aggregated form, without directly identifying any person. For the avoidance of doubt, this DPA will not apply to Service Data.
-

Part A: Personal Data protection obligations

4. Roles and responsibilities

4.1 Parties' Roles. Customer, as Controller, appoints TurnTo as a Processor to process the Personal Data described in **Annex A** on Customer's behalf.

4.2 Purpose Limitation. TurnTo shall process the Personal Data for the purposes described in **Annex A** and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law. The Agreement and this DPA sets out Customer's complete instructions to TurnTo in relation to the processing of the Personal Data and any processing required outside of the scope of these instructions will require prior written agreement between the parties.

4.3 Prohibited Data. Customer will not provide (or cause to be provided) any Sensitive Data to TurnTo for processing under the Agreement, and TurnTo will have no liability whatsoever for Sensitive Data that Customer may provide to TurnTo, whether accidental or intentional, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

(a) In a scenario where Customer provides TurnTo with Sensitive Data or Personal Data in excess of the data identified as needed in the contract terms during the initial Customer onboarding process, then TurnTo will communicate to the Customer and securely destroy any Sensitive Data unnecessary Personal Data obtained during onboarding.

(b) After the onboarding process, it is the Customers responsibility to monitor the Sensitive Data and Personal Data provided to TurnTo during daily operations, and to make requests to TurnTo update or delete any Sensitive Data or Personal Data that is not needed for the identified business purpose and/or as defined by the terms of the contract.

4.4 Description of Processing. A description of the nature and purposes of the processing, the types of Personal Data, categories of data subjects, and the duration of the processing are set out further in **Annex A**.

4.5 Compliance. Customer shall be responsible for ensuring that:

(a) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including EU Data Protection Legislation, in its use of the Services and its own processing of Personal Data (except as otherwise required by applicable law); and

(b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to TurnTo for processing in accordance with the terms of the Agreement and this DPA.

5. Security

5.1 Security. TurnTo shall implement appropriate technical and organizational measures to safeguard the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

5.2 Security Exhibit. The technical and organizational security measures which TurnTo shall have in place under the Agreement are defined in **Annex B** of this DPA.

6. International transfers

6.1 International Transfers. To the extent that TurnTo processes (or causes to be processed) any Personal Data originating from the EEA in a country that has not been designated by the European Commission as providing an adequate level of protection for Personal Data, the Personal Data

shall be deemed to have adequate protection (within the meaning of EU Data Protection Legislation) by virtue of TurnTo's self-certification to the Privacy Shield. TurnTo shall agree to apply the Privacy Shield Principles when processing (or causing to be processed) any EEA Data under this Agreement.

- 6.2 Privacy Shield Notifications. TurnTo agrees to notify Customer without undue delay if its self-certification to the Privacy Shield is withdrawn, terminated, revoked, or otherwise invalidated. In such a case, the parties shall cooperate in good faith to put in place such alternative data export mechanisms as are required under EU Data Protection Legislation to ensure an adequate level of protection for the Personal Data.

Part B: GDPR Obligations from May 25, 2018

7. Additional security

- 7.1 Confidentiality of processing. TurnTo shall ensure that any person that it authorizes to process the Personal Data shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).
- 7.2 Security Incidents. Upon becoming aware of a Security Incident, TurnTo shall notify Customer without undue delay and shall provide such timely information as Customer may reasonably require, including to enable Customer to fulfil any data breach reporting obligations, either under USA Federal law, or under EU Data Protection Legislation. TurnTo shall take appropriate and commercially reasonable steps to mitigate the effects of such a Security Incident on the Personal Data under this Agreement.

8. Sub-processing

- 8.1 Sub-processors. Customer agrees that TurnTo may engage TurnTo affiliates and third party sub-processors (collectively, "**Sub-processors**") to process the Personal Data on TurnTo's behalf. The Sub-processors currently engaged by TurnTo and authorized by Customer are available at **Annex C**. TurnTo shall maintain a list of its Sub-processors on its website at <https://www.turntonetworks.com/data-sub-processors/>. Customer shall be notified by TurnTo in advance of any new Sub-processor being appointed by changes to this website.
- 8.2 Objection to Sub-processors. Customer may object in writing to the appointment of an additional Sub-processor within five (5) calendar days after receipt of TurnTo's notice in accordance with the mechanism set out at Section 8.1 above. In the event that Customer objects on reasonable grounds relating to the protection of the Personal Data, then the parties shall discuss commercially reasonable alternative solutions in good faith. If no resolution can be reached, TurnTo will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected TurnTo service in accordance with the termination provisions of the Agreement.
- 8.3 Sub-processor obligations. Where a Sub-processor is engaged by TurnTo as described in this Section 8, TurnTo shall:
- (a) restrict the Sub-processor's access to Personal Data only to what is necessary to perform the subcontracted services;
 - (b) impose on such Sub-processors data protection terms that protect the Personal Data to the same standard provided for by this DPA; and
 - (c) remain liable for any breach of the DPA caused by a Sub-processor.

9. Cooperation

- 9.1 Cooperation and data subjects' rights. TurnTo shall, taking into account the nature of the

processing, provide reasonable assistance to Customer insofar as this is possible, to enable Customer to respond to requests from a data subject seeking to exercise their rights under EU Data Protection Legislation. In the event that such request is made directly to TurnTo, TurnTo shall promptly inform Customer of the same.

9.2 Data Protection Impact Assessments. TurnTo shall, to the extent required by EU Data Protection Legislation and at Customer's expense, taking into account the nature of the processing and the information available to TurnTo, provide Customer with commercially reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under EU Data Protection Legislation.

10. Information Security Risk Management

10.1 The parties acknowledge that TurnTo has a formal information security risk management process in place with policies, processes, internal controls, and procedures (e.g. safeguards) to protect systems and data. The parties also acknowledge that TurnTo utilizes consultants to assist with penetration testing, vulnerability assessments, and security assessments.

10.2 The parties further acknowledge that penetrating testing, vulnerability assessments, and security assessments are performed at least annually, and that TurnTo monitors risks on a daily basis within a risk register.

10.3 At Customer's written request, TurnTo will (on a confidential basis) provide Customer with a high-level summary status report of TurnTo's information security program including status of penetration testing, vulnerability assessments, security assessments, and compliance with GDPR.

10.4 At Customer's written request, TurnTo will (on a confidential basis) complete a security-focused questionnaire provided by Customer so that Customer can assess the extent and maturity of the security measures that TurnTo has in place to safeguard systems and data.

11. Deletion / return of data

11.1 Deletion or return of data: Upon termination or expiration of this Agreement, TurnTo shall at Customer's election, delete or return to Customer the Personal Data (including copies) in TurnTo's possession, save to the extent that TurnTo is required by any applicable law to retain some or all of the Personal Data.

[Signatures on Following Page]

Customer Execution:

Customer Legal Name: _____


Signed: _____

Name: _____

Title: _____

Date: _____

TurnTo Execution:

Signed:  _____

Name: George Eberstadt

Title: CEO

Date: 4-26-2018

ANNEX A

DESCRIPTION OF PROCESSING

Nature and purposes of processing

TurnTo is a US headquartered provider of cloud-based user-generated content (“UGC”) collection, management and analytics services. These services will consist primarily of solicitation of UGC submissions from purchasers (and those interested in purchasing) Customer’s goods and services through the use of email and website functionality; automated and manual evaluation of submissions for compliance with guidelines, and filter rules determined by the Customer; publishing and syndication of approved submissions to public web pages, applications, and 3rd party services determined by the customer; and providing Customer with reporting and analysis of the performance of the aforementioned services and nature of the UGC submissions.

Otherwise, the data processing will involve any such processing that is necessary for the purposes set out in the Agreement, the DPA, or as otherwise agreed between the parties.

Categories of data subjects

The concern about the transfer of personal data on data subjects includes:

- A user of Customer’s website(s) and application(s) in which TurnTo functionality is embedded for the purposes of users viewing and interacting with existing UGC, creating UGC, and behavioral tracking; or
- A purchaser of Customer goods and services that may or may not also be recipient of communications, such as email, for the purposes of soliciting UGC or being asked to interact with the TurnTo system; or
- A submitter of UGC on Customer’s website(s) and application(s); or
- A submitter of UGC on a Customer’s syndication partner’s website(s) and application(s); or
- An individual that is mentioned within the body of email communications, text notifications, or UGC submissions created by other individuals through the use of the TurnTo system

Categories of data

The personal data transferred concern the following categories of data for the data subjects:

- First and last name or initial (or nickname/screenshot), contact information (e-mail address and/or unique identifier); and
- Any other personal data that the Customer chooses to transmit, collect or display in its configured use of TurnTo's services.

The personal data transferred to TurnTo for processing is determined and controlled by the Customer in its sole discretion. As such, TurnTo has no control over the volume and sensitivity of personal data that is aggregated by the Customer.

Special categories of data (if appropriate)

TurnTo does not intentionally collect or process any special categories of data in the provision of its service. Under the Agreement, the Customer agrees not to provide special categories of data to TurnTo at any time.

Duration of processing

The personal data will be processed for the term of the Agreement, or as otherwise required by law or agreed between the parties.

ANNEX B

TURNT0 INFORMATION SECURITY PROGRAM

TurnTo hosts its systems and data at the service provider Amazon Web Services (AWS). AWS maintains a SOC 2 Type 2 report that covers the security, availability, and confidentiality principles for SOC reporting. The AWS SOC report is leveraged by TurnTo as evidence to demonstrate the comprehensive security policies, processes, internal controls, procedures, and reporting in place at AWS.

In addition to the SOC 2 report provided by the hosting provider AWS, TurnTo maintains its own internal information security program. TurnTo's information security program includes: policies, processes, internal controls, and procedures; all with the objective to safeguard the confidentiality, integrity, and availability of systems and data. TurnTo's information security program aligns with leading practice standards and frameworks including but not limited to: ISO 27000 series, NIST Cybersecurity Framework, other relevant NIST standards, as well as COBIT v5.

A sampling of domains covered within the TurnTo information security program include: policies and controls framework, security architecture, identity and access management, risk management, encryption, threat and vulnerability management, data classification and handling, change management, configuration management, logging and monitoring, incident management, vendor risk management, and security awareness training.

ANNEX C

TURNTO LIST OF SUB-PROCESSORS

Amazon Web Services, Inc.
Sendgrid, Inc.
Rebelmail, Inc.
GoodData Corporation
Mixpanel, Inc.
Box, Inc.