<u>**SENDGRID, INC.**</u>

**DATA PROCESSING ADDENDUM**

This Data Processing Addendum (this "**DPA**") is made as of the last date set forth on the signature page hereto (the "**Effective Date**") by and between SendGrid, Inc., a corporation organized and existing under the laws of the State of Delaware, U.S.A. ("**SendGrid**"), and the entity or person set forth on the signature page hereto ("**Customer**"), pursuant to the Agreement (as defined below).  This DPA has been pre-signed on behalf of SendGrid. This DPA will be void *ab initio*, with no force or effect, if the entity or person signing this DPA is not a party to an effective Agreement (as defined below) directly with SendGrid.  SendGrid 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 SendGrid 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 Terms of Service, OEM Agreement or SaaS Provider Agreement, as applicable, between the parties, in each case providing for the provision by SendGrid to Customer of the services described therein.

(b)      "**EEA**" means the European Economic Area (including the United Kingdom).

(c)      "**EU Data Protection Legislation**" means 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data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**") (as amended, replaced or superseded).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. and Swiss-U.S. Privacy Shield 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.

2.4    Notwithstanding anything in this DPA, SendGrid will have the right to collect, extract, compile, synthesize and analyze aggregated, non-personally identifiable data or information (data or information that does not identify Customer or any other entity or natural person as the source thereof) 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, recipients, bounce rates, or any other information regarding the email and other communications Customer, its end users or recipients generate and send using the Services. To the extent any Service Data is collected or generated by SendGrid, such data will be solely owned by SendGrid and may be used by SendGrid for any lawful business purpose without a duty of accounting to Customer or its recipients. For the avoidance of doubt, this DPA will not apply to Service Data.

## 3.    Roles and responsibilities

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

3.2    Purpose Limitation.  SendGrid 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 SendGrid 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.

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

3.4    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**.

3.5    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 SendGrid for processing in accordance with the terms of the Agreement and this DPA.

**4. Security**

4.1     <u>Security</u>.  SendGrid shall implement appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

4.2     <u>Security Exhibit.</u> The technical and organizational security measures which SendGrid shall have in place under the Agreement are set out at **Annex B** to this DPA.

**5. International transfers**

5.1     <u>International Transfers</u>. To the extent that SendGrid 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 SendGrid's self-certification to the Privacy Shield. SendGrid shall agree to apply the Privacy Shield Principles when processing (or causing to be processed) any EEA or Swiss Personal Data under this Agreement.

5.2     <u>Privacy Shield Notifications</u>. SendGrid 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.

**6. Additional security**

6.1     <u>Confidentiality of processing</u>.  SendGrid 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).

6.2     <u>Security Incidents</u>.  Upon becoming aware of a Security Incident, SendGrid 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 under EU Data Protection Legislation. SendGrid shall take appropriate and commercially reasonable steps to mitigate the effects of such a Security Incident on the Personal Data under this Agreement.

**7. Sub-processing**

7.1     <u>Sub-processors</u>. Customer agrees that SendGrid may engage SendGrid affiliates and third party sub-processors (collectively, "**Sub-processors**") to process the Personal Data on SendGrid's behalf. The Sub-processors currently engaged by SendGrid and authorized by Customer are available at https://sendgrid.com/policies/privacy/sub-processors/.  Customer shall be notified by SendGrid in advance of any new Sub-processor being appointed by changes to this website.

7.2     <u>Objection to Sub-processors</u>. Customer may object in writing to the appointment of an additional Sub-processor within five (5) calendar days after receipt of SendGrid's notice in accordance with the mechanism set out at Section 7.1 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, SendGrid will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected SendGrid service in accordance with the termination provisions of the Agreement.

7.3     <u>Sub-processor obligations</u>. Where a Sub-processor is engaged by SendGrid as described in this Section 7, SendGrid 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.

## 8.    Cooperation

8.1    <u>Cooperation and data subjects' rights</u>.  SendGrid 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 SendGrid, SendGrid shall promptly inform Customer of the same.

8.2    <u>Data Protection Impact Assessments</u>.  SendGrid 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 SendGrid, 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.

## 9.    Security reports and audits

9.1    The parties acknowledge that SendGrid uses external auditors to comprehensively assess the adequacy of its data processing against SOC standards, including the security of the systems and premises used by SendGrid to provide data processing services.

9.2    The parties further acknowledge that these audits:

(a)     are performed at least once each year;

(b)     are conducted by auditors selected by SendGrid, but otherwise conducted with all due and necessary independence and professionalism; and

(c)     are fully documented in an audit report that affirms SendGrid's controls meet the SOC standards against which they are assessed ("**Report**").

9.3    At Customer's written request, SendGrid will (on a confidential basis) provide Customer with a summary of the Report so that Customer can verify SendGrid's compliance with the audit standards against which it has been assessed, and this DPA.

9.4    SendGrid shall further provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm SendGrid's compliance with this DPA.

9.5    While it is the parties' intention ordinarily to rely on the provision of the Report and written responses provided under Sections 9.3 and 9.4 above to verify SendGrid's compliance with this DPA, SendGrid shall permit the Customer (or its appointed third party auditors) to carry out an audit of SendGrid's processing of Personal Data under the Agreement following a Security Incident suffered by SendGrid, or upon the instruction of a data protection authority. Customer must give SendGrid reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to SendGrid's operations. Any such audit shall be subject to SendGrid's security and confidentiality terms and guidelines.

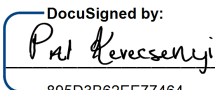**10.     Deletion / return of data**

10.1     <u>Deletion or return of data</u>:  Upon termination or expiry of the Agreement, SendGrid shall at Customer's election, delete or return to Customer the Personal Data (including copies) in SendGrid's possession, save to the extent that SendGrid is required by any applicable law to retain some or all of the Personal Data.
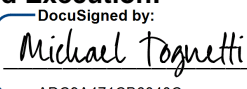
*[Signatures on Following Page]*

**SIGNED by the parties or their duly authorized representatives:**

**Customer Execution:**

Customer Legal Name: <u>The CodeDdraig Organisation</u>   SendGrid Account ID: <u>codedragon</u>

Signed: [ *Pal Kerecsenyi* ]

Name: <u>Pal Kerecsenyi</u>

Title: <u>Lead Developer</u>

Date: <u>8/20/2018</u>

**SendGrid Execution:**

Signed: [ *Michael Tognetti* ]

Name: Michael Tognetti

Title: SVP & General Counsel

Date: 5/25/2018

6

**ANNEX A**

**DESCRIPTION OF PROCESSING**

**Nature and purposes of processing**

SendGrid is a US headquartered provider of cloud-based transactional and marketing email delivery, management and analytics services. These services will consist primarily of sending and delivering e-mail communications on behalf of the Customer to its recipients and containing such content as are determined by the Customer in its sole discretion. SendGrid will also provide the Customer with analytic reports concerning the e-mail communications it sends on the Customer's behalf.

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 personal data transferred concern any data subject who is a sender, recipient or copy recipient of an email which the Customer instructs SendGrid to deliver and manage.

Data subjects may also include individuals who are mentioned within the body of emails sent by the Customer using SendGrid's services.

**Categories of data**

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

- Sender, recipient and copy recipient identification information (first and last name), contact information (address, telephone number (fixed and mobile), e-mail address, fax number), employment information (job title); and

- Any other personal data that the Customer chooses to include within the body of an e-mail that it sends using SendGrid's services.

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

**Special categories of data (if appropriate)**

SendGrid 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 SendGrid 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**

**SENDGRID SECURITY MEASURES**

1. **Network-Level Controls**

   a. SendGrid will use host-based firewall(s) to protect hosts/infrastructure handling Personal Data. The firewall(s) must be able to effectively perform the following functions: stateful inspection, logging, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing.
   b. SendGrid will have network-based security monitoring for the segment(s) on which hosts handling Personal Data are logically located.
   c. SendGrid will assess network-level vulnerabilities and address critical vulnerabilities within 30 days.
   d. SendGrid will employ change management standards for network/infrastructure components handling Personal Data.

2. **Hosting Level Controls**

   a. SendGrid will implement operating system hardening for hosts/infrastructure handling Personal Data. Operating system hardening includes, but is not limited to, the following configurations: strong password authentication/use of keys, inactivity time-out, disabling or removal of unused or expired accounts and services, turning off unused ports, and log management. In addition, SendGrid will implement access control processes and restrict access to operating system configurations based on the least privilege principle.
   b. SendGrid will perform patch management on systems that host or handle Personal Data. SendGrid will implement critical patches within vendor recommended timeframes on systems that host or handle Personal Data, not to exceed 30 days after the patch is identified.
   c. SendGrid will implement specific controls to log activities of users with elevated access to systems that host or handle Personal Data.
   d. SendGrid will, at a minimum, assess system-level vulnerabilities on a monthly basis and address critical vulnerabilities within 30 days.
   e. SendGrid will employ a comprehensive antivirus or endpoint security solution for endpoints which handle Personal Data.
   f. Physical servers will be protected with appropriate physical security mechanisms, including but not limited to badged access, locked cages, secure perimeter, cameras, alarms, and enforced user provisioning controls.

3. **Application-Level Controls**

   a. SendGrid will maintain documentation on overall application architecture, process flows, and security features for applications handling Personal Data.
   b. SendGrid will employ secure programming guidelines and protocols in the development of applications processing or handling Personal Data.
   c. SendGrid will regularly perform patch management on applications that host or handle Personal Data. SendGrid will implement critical patches within vendor recommended timeframes on all applications that host or handle Personal Data, not to exceed 30 days.
   d. SendGrid will, at a minimum, assess application-level vulnerabilities on a monthly basis and address critical vulnerabilities within 30 days.
   e. SendGrid will perform code review and maintain documentation of code reviews performed for applications that host or handle Personal Data.
   f. SendGrid will employ change management standards for applications hosting or handling Personal Data.

4. **Data-Level Controls**

SendGrid will use strong encryption (TLS) for transmission of Personal Data that is considered Confidential Information. Data backups of Personal Data will be encrypted at rest and while in transit; however due to the dynamic nature of data in SendGrid's production environment, Personal Data in SendGrid's production databases will not be encrypted at rest.

5. **End User Computing Level Controls**

   a. SendGrid will employ an end point security or antivirus solution for end user computing devices that handle Personal Data.
   b. SendGrid will ensure that end user computing devices that handle Personal Data are encrypted.

6. **Compliance Controls**

   a. SendGrid will make a good faith effort to operate within the parameters of SendGrid's then-current Information Security Policy. This Policy will be provided to Customer in soft copy format upon request.
   b. Notwithstanding any of the foregoing, SendGrid will adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to, building access control, employee education and personnel security measures.