GENERAL DATA PROTECTION REGULATION COMPLIANT
DATA PROCESSING ADDENDUM
INSTRUCTIONS FOR CUSTOMERS

WHO SHOULD EXECUTE THIS DPA:

If you have determined that you qualify as a Data Controller under the General Data Protection Regulation (GDPR), and need a Data Processing Addendum (DPA) in place with vendors that process personal data on your behalf, we want to help make things easy for you.

Our GDPR compliant DPA is attached and ready for your signature in accordance with the instructions below**.**

HOW TO EXECUTE THIS DPA:

1. Customer must complete the information in the signature boxes and sign on Page 6.
2. The Customer should send the completed and signed DPA to **support@suggestgrid.com**
3. **SuggestGrid, Inc.** (hereinafter referred to as **"Processor"**) will sign the DPA and will send it back to the Customer.

Upon receipt of the validly completed DPA by the Customer, this DPA will become legally binding.

DATA PROCESSING ADDENDUM

This Data Processing Addendum (DPA), is an addendum to and forms part of the Terms of Service (**"the Agreement"**) available at suggestgrid.com/terms. The purpose of this DPA is to reflect the Processor's and Customer's agreement with regard to the Processing of Personal Data by Processor on behalf of Customer in order to provide Processor Services to Customer and members of Customer's organization. Each of Processor and Customer may be referred to herein as a **"party"** and together as the **"parties"**.

1. Definitions

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Customer Data” means what is defined in the Agreement as “Your Data”.

“Data Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Data Processor” means the entity which processes Personal Data on behalf of the Data Controller.

“Data Protection Laws” means the GDPR and, and to the extent applicable, the data protection or privacy laws of any other country.

“Data Subject” means a natural person whose personal data is processed by a controller or processor.

“EU Model Clauses” means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection as approved by the European Commission pursuant to Decision C (2010)593.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27 April 2016 on the protection of natural persons with regards to the Processing of personal data and on the free movement of such data as applicable as of 25 May 2018, as may be amended from time to time.

“Personal Data” means any information relating to an identified or identifiable natural person Data Subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Processing” means any operation or set of operations which is performed on personal data whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

“Request” means a written request from a Data Subject to exercise his/her specific data subject rights under the Data Protection Laws in respect of Personal Data.

“Sub-processor” means any Data Processor engaged by Processor to process Customer Data on its behalf.

2. Processing

2.1. Role of the Parties: The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller, and Processor is the Data Processor.

2.2. Customer Processing of Personal Data: Customer shall, in its use of the Processor Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. Processing of Personal Data: Processor shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes:

2.3.1. Processing in order to provide Services to the Customer;

2.3.2. Processing initiated by Authorized Users in their use of the Services; and

2.3.3. Processing to comply with other documented reasonable instructions provided by Customer (e.g. support ticket) where such instructions are consistent with the terms of the Agreement.

3. Rights of Data Subjects

3.1. Corrections: To the extent Customer, in its use of the Service, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, Processor shall comply with any commercially reasonable Request by Customer to facilitate such actions to the extent Processor is legally permitted to do so.

3.2. Data Subject Requests: Processor shall, to the extent legally permitted, promptly notify Customer if it receives a Request from a Data Subject for access to, correction, amendment, or deletion of that person's Personal Data. Processor shall not fulfill any such Data Subject Request without Customer's prior written consent except to confirm that the Request relates to Customer. Processor shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use or receipt of the Services.

4. Processor Personnel

Processor shall take reasonable steps to ensure that access to the Controller Personal Data is limited on a need to know/access basis, and that all Processor personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Customer's Personal Data.

5. Sub-processors

5.1. Data Protection: Processor shall agree on substantially similar data protection obligations as set out in this DPA on any Sub-processor processing Customer's Personal Data.

5.2. Right of Information: Customer acknowledges and agrees that Processor may engage third-party Sub-processors in connection with the provision of the Services. A list of current Sub-processors can be provided upon written request.

5.3. Change of Sub-processors: The Processor will notify the Customer of any intended changes concerning the addition or replacement of Sub-processors. If the Customer legitimately objects to the addition of a Sub-processor within 30 days of the notification and the Processor cannot reasonably accommodate the Customer's objection, the Processor will notify the Customer. The Customer may terminate the Services by providing providing the Processor with a written notice within 30 days of the Provider's notice. The Provider will refund a prorated portion of any pre-paid charges for the period after such termination date.

6. Security

Processor shall maintain appropriate technical and organizational measures for the protection of the security, confidentiality and integrity of Personal Data.

7. Security Breaches

Processor maintains security incident management policies and procedures and shall, to the extent permitted by law, notify Customer without undue delay of any actual unauthorized disclosure of Customer Personal Data, by Processor or its Sub-processors of which Processor becomes aware (a "Security Breach") and provide details of the Security Breach to the Customer. To the extent such Security Breach is caused by a violation of the requirements of this DPA by Processor, Processor shall identify and remediate the cause of such Security Breach.

8. Data Transfers

Processor may Process Personal Data anywhere in the world where Processor or its Sub-processors maintain data Processing operations. Processor shall at all times provide an adequate level of protection for the Personal Data Processed, in accordance with the requirements of this DPA.

9. Deletion of Customer Personal Data

Processor shall delete Customer Personal Data in accordance with Processor's procedures and Data Protection Laws and consistent with the terms of the Agreement.

10. Audits

10.1. Audit Rights: Subject to Sections 10.2 and 10.3 below, Processor shall make available to a reputable auditor mandated by Customer in coordination with Processor, upon prior written request, such information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Processor, provided that such third-party auditor shall be subject to confidentiality obligations.

10.2. Scope of Audits: Provisions of information and audits are and shall be at Customer's sole expense, and may only arise under Section 10.1 above to the extent that audit rights meeting the relevant requirements of the applicable Data Protection Laws and agreements between the Processor and the Customer, including the Agreement. In any event, all audits or inspections shall be subject to the terms of the Agreement, and to Processor's obligations to third parties, including with respect to confidentiality.

10.3. Audit Terms: Customer shall give Processor reasonable prior written notice of any audit or inspection to be conducted under Section 10.1 above and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Customer and Processor shall mutually agree upon the scope, timing and duration of the audit or inspection in addition to the reimbursement rate for which Customer shall be responsible. Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1. to any individual unless he or she produces reasonable evidence of identity and authority;

10.3.2. if Processor was not given a written notice of such audit or inspection at least 2 weeks in advance;

10.3.3. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to Processor that this is the case before attendance outside those hours begins; or

10.3.4. for premises outside the Processor's control (such as Sub-processor premises)

10.3.5. for the purposes of more than one (1) audit or inspection, in respect of each Processor, in any calendar year, except for any additional audits or inspections which:

10.3.5.1. Customer reasonably considers necessary because of genuine concerns as to Processor's compliance with this DPA; or

10.3.5.2. Customer is required to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Customer has identified its concerns or the relevant requirement or request in its prior written notice to Processor of the audit or inspection.

11. Cooperation and Assistance

Processor shall provide reasonable assistance, information and cooperation to the Customer to ensure compliance with the Customer's obligations under Data Protection Laws.

12. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement.

This Data Processing Addendum is entered into and becomes a binding part of the Agreement with effect from the later date set out below. The parties' authorized signatories have duly executed this DPA:

PROCESSOR	**CUSTOMER**
Entity Legal Name:	Entity Legal Name:
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date: