

Data Processing Addendum

This Data Processing Addendum (the “**DPA**”) is made by and between Sigstr, Inc. a company incorporated under the laws of Delaware, having its principal place of business at 20 N Meridian Street, 4th Floor, Indianapolis, IN 46204 (“**Sigstr**”) and [CUSTOMER NAME AND ADDRESS], (“**Customer**”) (each a “**Party**” and together the “**Parties**”).

BACKGROUND

This DPA Addendum governs the processing of personal data by Sigstr and its approved sub-contractors for and on behalf of Customer, according to Customer’s instructions, and serves to supplement services as agreed in the respective Agreement. As part of the provision of Services by Sigstr, Personal Data may be transferred by the Customer to Sigstr.

In the course of providing certain data processing services ("Services") pursuant to the Agreement, Sigstr may process Customer Data as a Processor on behalf of Customer. This DPA Addendum is designed to ensure that Sigstr processes Customer Data in accordance with applicable data protection and privacy laws.

Parties hereby agree as follows:

1. **Definitions.**

"Data Controller" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Customer is the controller.

"Data Processor" means the entity processing Personal Data on behalf of the Data Controller. Sigstr, Inc. is the Data Processor.

"Data Protection Rules" means the relevant national laws that apply to the Processing of Personal Data in Data Protection Countries, including but not limited to any applicable privacy and information security laws and regulations that apply from time to time.

"EEA Data" means any Customer Data originating from the European Economic Area.

"GDPR" means the General Data Protection Regulation, (EU) 2016/679, that was adopted on April 27, 2016 and is enforceable as of May 25, 2018.

"Customer Data" means any Personal Data related to prospective or actual Customer personnel, Customers, business partners and/or suppliers for which Customer acts as a Data Controller.

"Personal Data" means any information relating to an identified or identifiable natural person (the "**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.

"Sub-processor" means an entity processing data on behalf of a Data Processor.

2. **Subject Matter and Purpose of this Addendum.** The Controller warrants that it will only provide Personal Data that is authorized for a permitted purpose to the Processor and the Controller is responsible for ensuring Controller’s invitees are aware of their obligations to protect Personal Data that is made available to them for a permitted purpose. The Processor shall Process, on behalf of the Controller, the Personal Data only within the scope and for the purposes detailed in Appendix 1 of this Addendum. This Addendum is intended to ensure adequate protection of Personal Data and information security and does not otherwise affect the rights and obligations between Parties under other agreements. In the event of any conflict between the provisions in this Addendum and the provisions set forth in the AGREEMENT, the provision or provisions of this Addendum will prevail.

3. **Term.** This Addendum is effective as of the date of execution and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of the Agreement.
4. **Relationship of the Parties.** Sigstr processes Customer Data as a Controller in the performance of its operations. Sigstr is hereby appointed to process Customer Data as a Data Processor on behalf of Customer. Sigstr will Process the Personal Data provided by Customer solely in accordance with Customer's written instructions and the provisions contained in this Addendum.
5. **General Obligations of the Processor**
 - 5.1 Sigstr's GDPR Obligations. Sigstr undertakes to Process the Personal Data in accordance with applicable Data Protection Rules; specifically, with respect to Personal Data from the European Economic Area or Switzerland, in accordance with its obligations as a data processor. Sigstr will comply with the terms in this Section 6 by no later than May 25, 2018.
 - 5.2 Personal Data Transferred Or Communicated To Third-Parties. Sigstr will neither transfer nor communicate the Personal Data to third parties nor Process or use it for its own purposes, unless otherwise stipulated in this Addendum, the MSA, or other agreed upon exhibits and in accordance with the Data Protection Rules. Sigstr will only onward transfer Personal Data in strict compliance with the Data Protection Rules and upon the prior written approval of the Controller.
 - 5.3 Sub-processors. Sigstr shall notify Customer if Sigstr engages any further Sub-processors to process Customer Data.
 - 5.4 Sub-processor conditions. Supplier must impose by binding contract no less stringent data protection obligations upon any further Sub-processors it engages as those set out in this Addendum. Sigstr shall remain fully liable for any acts or omissions of the Sub-processor that cause damage to Customer or its Customers.
6. **Confidentiality and Information Security Standards**
 - 6.1 Confidentiality of processing. Sigstr shall ensure that any person that it authorizes to process the Customer Data (including its personnel, agents and sub-processors) shall be subject to a strict duty of confidentiality (whether a contractual or statutory duty) and shall not permit any person to process the Customer Data who is not under such duty of confidentiality.
 - 6.2 Security Incidents. Upon becoming aware of any Security Incident affecting Customer Data, Sigstr will notify Customer in writing (via email and status page) of the Security Incident within no more than seventy-two (72) hours, providing detailed information about the Security Incident. Sigstr will immediately take all appropriate steps to remedy or mitigate the effects and minimize any damage resulting from the Security Incident. Sigstr will provide Customer such further information or cooperation as Customer may reasonably request regarding the Security Incident.
 - 6.3 Third party communications. Unless prohibited by applicable law, Sigstr will promptly notify Customer in the event that it receives any communication, correspondence or complaint from an individual, regulator or any other body relating to its processing of Customer Data. Sigstr will not respond directly to any such communication, correspondence or complaint without Customer's prior written consent. Sigstr shall provide all reasonable assistance to enable Customer to respond to such communication, correspondence or complaint.

6.4 Data protection impact assessments. Sigstr shall provide all reasonable assistance as Customer may require to conduct data protection impact assessments and, if necessary, to consult with relevant data protection authorities about the processing of Customer Data.

7. Documentation and Audits.

7.1 Copies of external security certifications and audit report summaries. Sigstr shall, upon Customer's written request, provide copies of external security certifications, audit report summaries and/or other documentation reasonably required by Customer to verify Supplier's compliance with this DPA Addendum.

8. Deletion/Return of Customer Data. Upon termination of the Agreement, Sigstr will return or delete all Customer Data it processes for and on behalf of Customer, except: (a) where otherwise instructed by Customer (acting as a Controller); or (b) to retain copies to the extent required under applicable law. Customer shall specify whether Sigstr shall delete and/or return Customer Data upon termination of the Agreement. Sigstr will delete Customer data, unless otherwise specified.

9. Miscellaneous.

9.1 Except as amended herein, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA Addendum, the terms of this DPA Addendum will control.

9.2 Any claims brought under this DPA Addendum shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

IN WITNESS WHEREOF, the undersigned have executed this DPA Addendum by their duly authorized representatives

ACCEPTED AND AGREED TO:

Company: Sigstr, Inc.

By: *Brent Mackay*
Authorized Signature

Print Name: Brent Mackay

Title: Data Protection Officer

Date: 5/16/18

CUSTOMER:

By:
Authorized Signature

Print Name:

Title:

Date: