DATA PROCESSING ADDENDUM
for Conga Partnership Programs

This Data Processing Addendum (this "**DPA**") is entered into by and between Apttus Corporation and its Affiliates ("**Conga**"), on the one hand, and the Partner identified in the Conga Partner Program Agreement and its Affiliates ("**Partner**"), on the other hand (together, the "**Parties**") and forms a part of the Conga Partner Program Agreement, as separately executed by the Parties (the "**Agreement**"). This DPA forms an integral part of the Agreement and governs the data sharing between Partner and Conga.

The terms of this DPA prevail over any conflicting terms in the Agreement and in any other agreement(s) between the Parties, with the sole exception of the Standard Contractual Clauses, as defined below. Where the terms of this DPA conflict with the terms of an applicable module of the Standard Contractual Clauses, the terms of the applicable module of the Standard Contractual Clauses control.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

This DPA is designed to cover three different potential configurations for the exchange of Personal Data, as that term is defined below, between Conga and Partner. Taking into consideration the provisions of the Agreement and the nature of the relationship between the Parties, the Parties have designed this DPA to address:

- **Controller-to-Controller Configuration:** Where Partner and Conga share Personal Data with the intent that each Party will use the Personal Data, after receiving it from the other, for its own purposes, Partner and Conga are sharing such Personal Data as independent Controllers. For example, when Partner refers contact information on prospects to Conga, so that Conga may then use that contact information to market Conga Products to those prospects, Partner is engaged in a Controller-to-Controller transfer of Personal Data to Conga.
- **Controller-to-Processor Configuration:** Where Partner processes Personal Data exclusively on behalf of Conga, and according to Conga's instructions, in order to help Conga meet Conga's own objectives, Partner acts a Processor to Conga as a Controller. For example, if Conga provides Personal Data to Partner for the exclusive purpose of enabling Partner to resell Conga Products, Partner processes that Personal Data as a Processor to Conga as a Controller,
- **Processor-to-Sub-Processor Configuration:** Where Partner processes Personal Data exclusively on behalf of Conga, and according to Conga's instructions, in order to help Conga meet a Customer's objectives, Partner will be a Sub-Processor to Conga as a Processor, while the Customer will be the Controller. For example, if Conga provides Partner with access to Customer Personal Data, as defined below, so that Partner can assist Conga in providing a support service to the Customer, Partner will be a Sub-Processor to Conga as a Processor.
- **Joint Processor Configuration:** Conga and Partner may each be Processors of a Joint Customer's Personal Data and transfer such data to the other party for processing at the direction of the Joint Customer.

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.

"Applicable Data Protection Laws" means all laws applicable to the Processing of Personal Data contemplated by the Agreement, including, where applicable, (1) the U.S. Data Protection Laws, (2) the GDPR and the laws of non-EU EEA countries that have formally adopted the GDPR, (3) the UKGDPR, (4) the Swiss Federal Act on Data Protection ("Swiss FADP"); or (5) any other data protection laws applicable to the Processing of Personal Data hereunder. Where this DPA intends to refer to the data protection laws of a specific jurisdiction, it will designate that jurisdiction as a modifier (for example, "**UK Data Protection Laws**," or "**EEA Data Protection Laws**").

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et seq., and its implementing regulations, and, whenever applicable, the amendments to the CCPA contained within the California Privacy Rights Act.

"Controller" means an entity which determines the purposes and means of the Processing of Personal Data.

"Data Subject" means the Identifiable Natural Person to whom Personal Data relates.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation).

"**Identifiable Natural Person**" means 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.

"Joint Customer" means a customer of both Partner and Conga.

"Joint Customer Personal Data" means any Personal Data for which a Joint Customer acts as a Controller.

"Personal Data" means any data or information that relates to an Identifiable Natural Person, to the extent that such information is Processed by either Party pursuant to the Agreement. "**Customer Personal Data**" is Personal Data that Conga Processes as a Processor to a customer, and which Partner may Process as a Sub-Processor to Conga. Where this DPA intends to refer to a subset of Personal Data, the processing of which is regulated by the Applicable Data Protection Laws of a particular jurisdiction, it will designate that jurisdiction as a modifier (for example, "**EEA Personal Data**," or "**UK Personal Data**").

"**Security Incident**" means a suspected or actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"Processor" means an entity which Processes Personal Data on behalf of a Controller.

"**Restricted Transfer of Personal Data**" means any transfer of Personal Data to a jurisdiction other than the jurisdiction in which the Data Subjects to whom the Personal Data relates were located at the time of collection, or to an international organization in a jurisdiction other than the jurisdiction in which the Data Subjects to whom the Personal Data relates were located at the time of collection, including data storage on foreign servers or access to such stored data from a foreign jurisdiction, but only to the extent that such transfer is regulated by Applicable Data Protection Laws.

"Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

"Standard Contractual Clauses" or "SCCs" means the clauses set forth in the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Sub-Processor" means an entity which Processes Personal Data on behalf of a Processor, consistent with directions provided to that Processor by a Controller and flowed down to the Sub-Processor through a written contract.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

"Sensitive Data" means data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

"**UKGDPR**" means the GDPR as implemented or adopted under the laws of the United Kingdom.

"**U.S. Data Protection Laws**" means all laws and regulations of the United States of America, including the CCPA, applicable to the Processing of Personal Data under the Agreement.

2. SCOPE AND APPLICABILITY

2.1 **Controller-to-Controller Configuration.** When the Parties act as independent Controllers with respect to the Processing of Personal Data, the provisions of Sections 3 and 6 through 9 of this DPA shall govern such Processing, and the provisions of Section 10.1.1 of this DPA shall govern any Restricted Transfers of Personal Data.

2.2 **Controller-to-Processor Configuration.** When Conga is a Controller and Partner is a Processor, the provisions of Sections 4, 6 through 9, and 11 of this DPA shall govern the associated Processing, and the provisions of Section 10.1.2 of this DPA shall govern any Restricted Transfers of Personal Data.

2.3 **Processor-to-Sub-Processor Configuration.** When Conga is a Processor to a customer and Partner is a Sub-Processor to Conga, the provisions of Sections 5, 6 through 9, and 11 of this DPA shall govern the associated Processing, and the provisions of Section 10.1.3 of this DPA shall govern any Restricted Transfers of Personal Data.

2.4 **Joint Processor Scenarios.** Each party, to the extent that it, along with the other party, acts as a Processor with respect to Joint Customer Personal Data, will (i) comply with the instructions and restrictions set forth in its own agreement(s) with the Joint Customer; and (ii) reasonably cooperate with the other party to enable the exercise of data subject rights as set forth in Applicable Data Protection Laws. The parties both acknowledge and agree that in such a Joint Processor Scenario, each party is acting as a Processor for the Joint Customer and neither party is engaging the other as a Sub-processor, and therefore each party is responsible for entering into its own data processing agreement with the Joint Customer. Where necessary, Restricted Transfers of Personal Data between and among the parties as Joint Processors shall be pursuant to Module Three of the Standard Contractual Clauses, as incorporated and implemented in Sections 10.1.3(i)-(iii), except that either party may be the data exporter or the data importer, and neither party shall be considered a Sub-processor.

3. CONTROLLER-TO-CONTROLLER CONFIGURATION

3.1 When Processing Personal Data as an independent Controller, each Party represents and warrants to the other Party that:

3.1.1 All Personal Data has been and will be collected and otherwise Processed in compliance with Applicable Data Protection Laws.

3.1.2 It will independently determine its obligations under Applicable Data Protection Laws, and it shall be responsible for its own compliance with those obligations.

3.1.3 It will not further Process Personal Data, or allow any Processor to further Process Personal Data, in a manner that is incompatible with the purposes for which the Controller disclosing the Personal Data originally collected it, without disclosing such further use to the Data Subject(s), ensuring that an appropriate lawful basis for such further use exists, and ensuring that such further use is otherwise compliant with Applicable Data Protection Laws.

3.1.4 It will Process Personal Data only on lawful grounds pursuant to Article 6 of the GDPR, where applicable, and as further limited by Article 9 of the GDPR, where applicable, or the relevant provisions of any Applicable Data Protection Laws, as the case may be.

3.1.5 It will only engage a Processor to Process Personal Data on its behalf or share Personal Data with a third-party Controller if that Processor or third-party Controller provides sufficient guarantees to that Party, by way of a written contract, that it will duly account for all requirements of any Applicable Data Protection Laws, as the case may be.

3.1.6 It will be solely responsible for responding to requests it receives related to the exercise of rights of the Data Subjects, as provided for by Applicable Data Protection Laws, with regard to the Personal Data Processed by that Party, and it will provide, upon the request of the other Party, prompt and reasonable assistance, where legally required or reasonably expected, to enable both Parties to comply with such Data Subject requests.

3.1.7 It will comply with Section 10.1.1 of this DPA with respect to Restricted Transfers of Personal Data.

4. CONTROLLER-TO-PROCESSOR CONFIGURATION

4.1 Roles of the Parties. This Section 4 applies when Conga is a Controller and Partner is a Processor to Conga.

4.2 Purposes of Processing. When Partner acts as a Processor to Conga, Partner shall Process Personal Data solely according to the documented instructions of Conga, and not for any other purpose. The purpose of such Processing shall be to provide Conga with the service contemplated by such documented instructions.

4.3 Details of the Processing. The subject matter of the Processing of Personal Data by Partner is as described above, in Section 4.2. The duration of the Processing, the nature of the Processing, the types of Personal Data, and the categories of Data Subjects shall be as set forth in Attachment A.

4.4 Partner's Obligations as Processor. When Partner acts as Conga's Processor, Partner shall:

4.4.1 Comply with all Applicable Data Protection Laws in the Processing of Personal Data;

4.4.2 Not Process Personal Data other than on the documented instructions of Conga, including with regard to transfers of Personal Data to a third country or an international organization, unless such Processing is required by Applicable Data Protection Laws to which Partner is subject, in which case Partner shall, to the extent permitted by Applicable Data Protection Laws, inform Conga of that legal requirement before performing the relevant act of Processing;

4.4.3 Immediately inform Conga if, in Partner's opinion, a documented instruction from Conga infringes any Applicable Data Protection Laws; and

4.4.4 Ensure that all persons authorized to Process the Personal Data on behalf of Partner have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.5 Control over the Personal Data. Conga will retain all authority and control over the Personal Data. Partner must therefore always grant Conga access to the Personal Data immediately at Conga's request.

4.6 Duty of assistance and information. Partner will ensure that Conga is able to comply with the Applicable Data Protection Laws with respect to the Processing of Personal Data, and Partner will provide all relevant assistance to Conga, including in the preparation of any necessary DPIAs or prior consultations.

4.7 Data Subject Requests. Partner shall promptly, and in no event later than within forty-eight (48) hours of receipt, notify Conga if Partner receives any request from a Data Subject to exercise any right permitted by Applicable Data Protection Laws with respect to Customer Personal Data, including but not limited to, where applicable, the right of access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "**Data Subject Request**"). Partner shall take no further action with respect to any such Data Subject Request unless instructed by Conga.

4.8 Appointment of Sub-Processors. Conga acknowledges and agrees that (a) Partner's Affiliates may be retained as Sub-Processors through written agreement with Partner and (b) Partner and Partner's Affiliates respectively may engage third-party Sub-Processors with Conga's specific prior authorization. As a precondition to permitting a third-party Sub-Processor to Process Personal Data, Partner or a Partner Affiliate will enter into a written agreement with each Sub-Processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processor.

4.9 List of current Sub-Processors and notification of new Sub-Processors. A current list of Partner's relevant Sub-Processors, including the identities of those Sub-Processors, their locations, and a description of such processing, shall either be provided to Conga prior to signature of the Agreement, or, to the extent Partner does not provide such list, Partner represents that there are no applicable Sub-Processors for Partner's processing.

4.10 Authorization process for New Sub-Processors. Before adding any new Sub-Processor, Partner shall provide Conga with written notice of its intentions, including the details of the intended Sub-Processor appointment. Upon receipt of such written notice, Conga shall have thirty (30) business days to decide whether to approve the new Sub-Processor. If Conga objects to the proposed new Sub-Processor, Partner shall not permit such entity to Process any Customer Personal Data. If Partner cannot honor its commitments under the Agreement without the use of a Sub-Processor to which Conga objects, Conga may terminate the Agreement without penalty by providing written notice to Partner.

4.11 Liability. Partner shall be liable for the acts and omissions of its Sub-Processors to the same extent Partner would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

5. PROCESSOR-TO-SUB-PROCESSOR CONFIGURATION

5.1 Roles of the Parties. This Section 5 applies when Conga is a Processor to a Customer and Partner is a Sub-Processor to Conga.

5.2 Contractual Arrangement. Conga has concluded a contract with a Customer as Controller ("**Main Contract**"), in connection with which Conga Processes Customer Personal Data under a separate data processing agreement ("**Main DPA**"). Conga may from time subcontract certain services required under the Main Contract to Partner. If so, as permitted by the Main DPA, Conga will give Partner access to Customer Personal Data, and Partner will process that Customer Personal Data in the course of performing services for Conga. As a Sub-Processor, Partner will comply with and be bound by all directions and instructions of the Customer, flowed down from the Main DPA through this DPA to Partner. Partner shall have no direct contact with Customer, and Partner shall receive Processing instructions only through Conga.

5.3 Purposes of Processing. As a Sub-Processor, Partner shall Process Customer Personal Data solely according to the documented instructions of Conga, and not for any other purpose. The purpose of such Processing shall be to assist Conga in meeting its obligations to the Customer under the Main Agreement and the Main DPA.

5.4 Details of the Processing. The subject matter of the Processing of Customer Personal Data by Partner is as described above, in Sections 5.2 and 5.3. The duration of the Processing, the nature of the Processing, the types of Personal Data, and the categories of Data Subjects shall be as set forth in Attachment A.

5.5 Partner's Obligations as Sub-Processor. When Partner acts as Conga's Sub-Processor, Partner shall:

5.5.1 Comply with all Applicable Data Protection Laws in the Processing of Customer Personal Data;

5.5.2 Not Process Customer Personal Data other than on the documented instructions of Conga, including with regard to transfers of Customer Personal Data to a third country or an international organization, unless such Processing is required by Applicable Data Protection Laws to which Partner is subject, in which case Partner shall, to the extent permitted by Applicable Data Protection Laws, inform Conga of that legal requirement before performing the relevant act of Processing;

5.5.3 Immediately inform Conga if, in Partner's opinion, a documented instruction from Conga infringes any Applicable Data Protection Laws; and

5.5.4 Ensure that all persons authorized to Process the Customer Personal Data on behalf of Partner have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.6 Control over the Personal Data. As between Conga and Partner, Conga will retain control over the Customer Personal Data. Partner must therefore always grant Conga access to the Customer Personal Data immediately at Conga's request.

5.7 Duty of assistance and information. Partner will ensure that Conga is able to comply with the Applicable Data Protection Laws and its corresponding obligations under the Main DPA, and Partner will provide assistance to Conga, including in the preparation of any necessary DPIAs or prior consultations, to enable Conga to do so.

5.8 **Data Subject Requests.** Partner shall promptly, and in no event later than within forty-eight (48) hours of receipt, notify Conga if Partner receives any request from a Data Subject to exercise any right permitted by Applicable Data Protection Laws with respect to Customer Personal Data, including but not limited to, where applicable, the right of access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "Data Subject Request"). Partner shall take no further action with respect to any such Data Subject Request unless instructed by Conga.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Partner has implemented and maintains technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk of the Processing. Partner shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in Attachment B. Partner regularly monitors compliance with these measures.

6.2 **Audit Rights.** Upon Conga's request, Partner shall make available to Conga (or Conga's independent third-party auditor) any and all requested information regarding Partner's compliance with the obligations set forth in this DPA. In addition, Partner shall allow for and contribute to audits by Conga (or Conga's independent third-party auditor) of Partner's procedures relevant to the protection of Personal Data. Before the commencement of any such audit, Conga and Partner shall mutually agree upon the scope, timing, and duration of the audit. Conga shall promptly notify Partner with information regarding any non-compliance discovered during an audit, and Partner shall use commercially reasonable efforts to address any non-compliance.

7. PERSONAL DATA INCIDENT MANAGEMENT AND SECURITY INCIDENT NOTIFICATION

7.1 **Government Requests.** Unless prohibited by law, Partner must inform Conga immediately and prior to providing any Personal Data, including any Customer Personal Data, if a competent government authority, including a Supervisory Authority, has made a request for the provision of such Personal Data.

7.2 **Incident Notification.** Partner shall notify Conga promptly after discovering, but in no event later than twenty-four (24) hours after discovering, any Security Incident. Partner shall provide cooperation and assistance to Conga in identifying the cause of such Security Incident and shall take reasonable steps to remediate the cause.

7.3 **Procedures.** If a Security Incident occurs, Partner's notice to Conga shall include a description of the nature of the Security Incident, the categories of Data Subjects, the number of Data Subjects, the anticipated consequences of the Security Incident and the measures adopted to remedy the consequences. Partner must also cooperate fully with Conga and follow Conga's instructions in relation to the Security Incident. This is to enable Conga to conduct an adequate investigation into the Security Incident, to formulate a correct response and to take appropriate follow-up steps regarding the Security Incident. Partner will ensure that Conga is able to comply with the Applicable Data Protection Laws regarding the Security Incident, including reporting in a timely (within the timeframe set in the Applicable Data Protection Laws) and accurate manner to the Supervisory Authority designated in the applicable legislation, where necessary, to customers and other contracting partners, where necessary, and to the Data Subjects, where necessary. This means that Partner must report every Security Incident to Conga, regardless of whether it constitutes a Security Incident that is required to be reported to the Supervisory Authority.

7.4 **Continuing Obligation.** After making an initial notification in compliance with Sections 7.2 and 7.3 above, Partner will keep Conga informed of any new developments concerning the Security Incident and of the measures Partner is taking to limit the consequences of the Security Incident and to prevent recurrence.

7.5 **Reporting Decisions.** Where the Parties are independent Controllers with respect to any Personal Data involved in a Security Incident, each Party shall determine and adhere to its own reporting obligations. However, where Partner is a Processor or Sub-Processor to Conga, then, as between Conga and Partner, Conga will exclusively determine whether to report the Security Incident to the Supervisory Authority, to any Conga Customers or other contracting partners, and/or to the Data Subject(s). Partner will not report the Security Incident to any individual or entity other than Conga. Partner is not permitted to make any statements to third parties and/or the media. Any questions must be forwarded to Conga.

8. RETURN AND DELETION OF PERSONAL DATA

8.1 To the extent Partner Processes Personal Data pursuant to the Agreement as a Processor or Sub-Processor to Conga, upon termination of the Agreement, Partner shall, upon Conga's election, return all Personal Data in Partner's possession to Conga or securely destroy such Personal Data and demonstrate to the satisfaction of Conga that it has taken such measures.

9. LIABILITY AND INDEMNIFICATION

9.1 Each Party's 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 provisions of the Agreement limiting liability, and any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and all DPAs together.

9.2 Partner's obligation to indemnify Conga against the consequences of Partner's breach of any provision of this DPA shall be as set forth in the Agreement.

10. RESTRICTED TRANSFERS OF PERSONAL DATA

10.1 The Parties hereby acknowledge and agree that all Restricted Transfers of Personal Data that take place in connection with the Parties' performance of their obligations under the Agreement will be conducted in accordance with the requirements of the Applicable Data Protection Laws.

10.1.1 Controller-to-Controller Configuration. Unless the destination country has received an adequacy decision from the European Commission or a similar competent authority, all Controller-to-Controller Restricted Transfers of Personal Data subject to the GDPR, the UKGDPR, or the Swiss FADP shall take place pursuant to the Standard Contractual Clauses, or their UK or Swiss-adapted counterparts, as further set forth herein.

(i) **Restricted Transfers of EEA Personal Data.** Restricted Transfers of EEA Personal Data shall be conducted pursuant to the Standard Contractual Clauses, or SCCs, as defined above, unless the receiving jurisdiction has received an adequacy decision from the European Commission. Where applicable, this DPA therefore incorporates the SCCs by reference, and the Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety, including the associated annexes.

- With respect to any Controller-to-Controller Restricted Transfers of EEA Personal Data, the Parties agree to implement Module One of the SCCs, with the Party sending the Personal Data as the Data Exporter and the Party receiving the Personal Data as the Data Importer.
- The contents of Annex I of the SCCs are included within Attachment A. The contents of Annex II are included within Attachment B.
- The Parties further agree to the following:
  - Clause 7: The Parties choose not to include the optional docking clause.
  - Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
  - Clause 13: Where the Data Exporter is established in an EU member state, the

competent Supervisory Authority shall be the Supervisory Authority for that member state. Where the Data Exporter is not established within an EU member state, but the Data Exporter falls within the territorial scope of the GDPR pursuant to Article 3(2) and has appointed a Data Protection Representative, the competent Supervisory Authority shall be the Supervisory Authority in the member state where the Data Exporter's Data Protection Representative is established. In all other cases, the Irish Data Protection Commission will be the competent Supervisory Authority.

- Clause 17: The clauses shall be governed by the laws of the Republic of Ireland.
- Clause 18: The Parties agree that any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland.

(ii) **Restricted Transfers of Swiss Personal Data.** Restricted Transfers of Swiss Personal Data shall be conducted pursuant to the SCCs, which have been adopted for use by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") with certain modifications. Where applicable, this DPA therefore incorporates the SCCs by reference, and the Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety, including the associated annexes. The Parties incorporate and adopt the SCCs as to Restricted Transfers of Swiss Personal Data in exactly the same manner set forth in Section 10.1.1(i) above, with the following two caveats:

- Clause 13: Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Swiss data subjects from applying to the FDPIC for relief.
- Clause 18: The Parties' selection of forum may not be construed as forbidding data subjects in Switzerland from suing for their rights in Switzerland.

(iii) **Restricted Transfers of UK Personal Data.** Restricted Transfers of UK Personal Data shall be conducted pursuant to the SCCs, along with any necessary modifications and addenda to make the SCCs applicable to transfers of UK Personal Data (including the adoption and incorporation by reference of the UK transfer addendum available at https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf) ("**UK Transfer Addendum**"). The information required by Table 1 of the UK Transfer Addendum appears within Attachment A to this DPA. Beyond that, the Parties incorporate and adopt the SCCs as to Restricted Transfers of UK Personal Data in exactly the same manner set forth in Section 10.1.1(i) above, with the following three caveats:

- Clause 13: The UKICO shall be the competent Supervisory Authority.
- Clause 17: The SCCs, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.
- Clause 18: The Parties agree that any dispute arising from the SCCs or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

10.1.2 Controller-to-Processor Configuration. Unless the destination country has received an adequacy decision from the European Commission or a similar competent authority, all Controller-to-Processor Restricted Transfers of Personal Data from Conga to Partner subject to the GDPR, the UKGDPR, or the Swiss FADP shall take place pursuant to the Standard Contractual Clauses, or their UK or Swiss-adapted counterparts, as further set forth herein.

(i) **Restricted Transfers of EEA Personal Data.** Restricted Transfers of EEA Personal Data shall be conducted pursuant to the Standard Contractual Clauses, or SCCs, as defined above, unless the receiving jurisdiction has received an adequacy decision from the European Commission. Where applicable, this DPA therefore incorporates the SCCs by reference, and the Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety, including the associated annexes.

- With respect to any Controller-to-Processor Restricted Transfers of EEA Personal Data, the Parties agree to implement Module Two of the SCCs, with Conga as the Data Exporter and Partner as the Data Importer.
- The contents of Annex I of the SCCs are included within Attachment A. The contents of Annex II are included within Attachment B.
- The Parties further agree to the following:
  - Clause 7: The Parties choose not to include the optional docking clause.
  - Clause 9(a): The Parties choose Option 1, "Specific Prior Authorization," and thirty (30) days. The procedures for designation and notification of new Sub-Processors are set forth in more detail in Sections 4.8 through 4.10.
  - Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
  - Clause 13: The Irish Data Protection Commission will be the competent Supervisory Authority.
  - Clause 17: The clauses shall be governed by the laws of the Republic of Ireland.
  - Clause 18: The Parties agree that any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland.

(ii) **Restricted Transfers of Swiss Personal Data.** Restricted Transfers of Swiss Personal Data shall be conducted pursuant to the SCCs, which have been adopted for use by the FDPIC with certain modifications. Where applicable, this DPA therefore incorporates the SCCs by reference, and the Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety, including the associated annexes. The Parties incorporate and adopt the SCCs as to Restricted Transfers of Swiss Personal Data in exactly the same manner set forth in Section 10.1.2(i) above, with the following two caveats:

- Clause 13: Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Swiss data subjects from applying to the FDPIC for relief.
- Clause 18: The Parties' selection of forum may not be construed as forbidding data subjects in Switzerland from suing for their rights in Switzerland.

(iii) **Restricted Transfers of UK Personal Data.** Restricted Transfers of UK Personal Data shall be conducted pursuant to the SCCs, along with any necessary modifications and addenda to make the SCCs applicable to transfers of UK Personal Data (including the UK Transfer Addendum). The information required by Table 1 of the UK Transfer Addendum appears within Attachment A to this DPA. Beyond that, the Parties incorporate and adopt the SCCs as to Restricted Transfers of UK Personal Data in exactly the same manner set forth in Section 10.1.2(i) above, with the following three caveats:

- Clause 13: The UKICO shall be the competent Supervisory Authority.
- Clause 17: The SCCs, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.
- Clause 18: The Parties agree that any dispute arising from the SCCs or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

10.1.3 Processor-to-Sub-Processor Configuration. Unless the destination country has received an adequacy decision from the European Commission or a similar competent authority, all Processor-to-Sub-Processor Restricted Transfers of Personal Data from Conga to Partner subject to the GDPR, the UKGDPR, or the Swiss FADP shall take place pursuant to the Standard Contractual Clauses, or their UK or Swiss-adapted counterparts, as further set forth herein.

(i) **Restricted Transfers of EEA Personal Data.** Restricted Transfers of EEA Personal Data shall be conducted pursuant to the Standard Contractual Clauses, or SCCs, as defined above, unless the receiving jurisdiction has received an adequacy decision from the European Commission. Where applicable, this DPA therefore incorporates the SCCs by reference, and the Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety, including the associated annexes.

- With respect to any Processor-to-Sub-Processor Restricted Transfers of EEA Personal Data, the Parties agree to implement Module Three of the SCCs, with Conga as the Data Exporter and Partner as the Data Importer.
- The contents of Annex I of the SCCs are included within Attachment A. The contents of Annex II are included within Attachment B.
- The Parties further agree to the following:
  - Clause 7: The Parties choose not to include the optional docking clause.
  - Clause 9(a): The Parties choose Option 1, "Specific Prior Authorization," and thirty (30) days.
  - Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
  - Clause 13: The Irish Data Protection Commission will be the competent Supervisory Authority.
  - Clause 17: The clauses shall be governed by the laws of the Republic of Ireland.
  - Clause 18: The Parties agree that any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland.

(ii) **Restricted Transfers of Swiss Personal Data.** Restricted Transfers of Swiss Personal Data shall be conducted pursuant to the SCCs, which have been adopted for use by the FDPIC with certain modifications. Where applicable, this DPA therefore incorporates the SCCs by reference, and the Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety, including the associated annexes. The Parties incorporate and adopt the SCCs as to Restricted Transfers of Swiss Personal Data in exactly the same manner set forth in Section 10.1.3(i) above, with the following two caveats:

- Clause 13: Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Swiss data subjects from applying to the FDPIC for relief.
- Clause 18: The Parties' selection of forum may not be construed as forbidding data subjects in Switzerland from suing for their rights in Switzerland.

(iii) **Restricted Transfers of UK Personal Data.** Restricted Transfers of UK Personal Data shall be conducted pursuant to the SCCs, along with any necessary modifications and addenda to make the SCCs applicable to transfers of UK Personal Data (including the UK Transfer Addendum). The information required by Table 1 of the UK Transfer Addendum appears within Attachment A to this DPA. Beyond that, the Parties incorporate and adopt the SCCs as to Restricted Transfers of UK Personal Data in exactly the same manner set forth in Section 10.1.3(i) above, with the following three caveats:

- Clause 13: The UKICO shall be the competent Supervisory Authority.
- Clause 17: The SCCs, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.
- Clause 18: The Parties agree that any dispute arising from the SCCs or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

11. UNITED STATES PROVISIONS

11.1 Relationship. The parties acknowledge and agree that, when Partner acts as a Sub-Processor or Processor to Conga as a Processor or Controller, as contemplated by Sections 4 and 5 this DPA, respectively, Partner is also a "Service Provider," for purposes of the CCPA, and Partner receives Personal Data pursuant to the business purpose of providing services to Conga in accordance with the Agreement.

11.2 Disclosure. When Partner acts as a Service Provider to Conga, Partner shall not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than for the specific purpose established by Conga, including retaining, using or disclosing Personal Data for a commercial purpose other than the purpose established by Conga; and (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Conga and Partner. Partner certifies that Partner understands the restrictions in this Section 11 and will comply with them in accordance with the requirements of Applicable Data Protection Laws, including, where relevant, the CCPA.

List of Attachments

Attachment A: Description of Processing Activities
Attachment B: Technical and Organizational Measures

ATTACHMENT A TO EXHIBIT E

Details of Processing

A. LIST OF PARTIES:

Partner:

Name:	The Partner identified in the Agreement and/or Order Form(s)/Statement(s) of Work and, all Affiliates of Partner.
Address:	Partner's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work.
Contact Person:	Partner's telephone number and email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work.
Activities Relevant to Transferred Data:	Use of Conga Products and/or Services, and/or participation in the Conga Partner Program and use of Conga Partner Community website.
Role:	Data Importer or Exporter (as an independent Controller); Data Importer (as a Processor or Sub-Processor); *see* Section 10 of the DPA for more details.

Conga:

Name:	Apttus Corporation
Address:	13699 Via Varra, Broomfield, CO 80020, USA
Contact Person:	Stephen Tam, Director of Security and Compliance, privacy@conga.com
Activities Relevant to Transferred Data:	Conga is a provider of enterprise cloud computing solutions and the Conga Partner Program, including the Conga Partner Community website, all of which Process Personal Data upon the instructions of the Partner and in accordance with the terms of the Agreement and this DPA.
Role:	Data Importer or Exporter (as an independent Controller); Data Exporter (when Partner is a Processor or Sub-Processor); *see* Section 10 of the DPA for more details.

B. DESCRIPTION OF TRANSFER:

Subject Matter of the Processing:	The subject matter of the Processing of Personal Data by Conga is the exchange of information, Services, and/or Products as defined in the Agreement.
Nature and Purpose of Processing:	The Processing is related to Conga's provision of SaaS solutions and information about SaaS solutions to Partner, Partner's referral of end customers to Conga, and/or Partner's marketing or implementation of Conga SaaS solutions to end customers, as further detailed in the Agreement. Conga and its Sub-processors will perform such acts of Processing of Personal Data as are necessary to the purpose of the Agreement, according to Partner's instructions, including but not limited to the transmission, storage, and other Processing of Personal Data submitted to Conga for the purpose of the Agreement.
Duration of Processing:	The Processing as described herein will continue for the duration of the Agreement and so long as Partner participates in Conga Partner Program and/or uses or accesses Conga Partner Community website.
Categories of Data Subjects:	The parties may exchange Personal Data for the purpose of the Agreement,

	which may include Personal Data relating to the following categories of Data Subjects: • Prospects, customers, business partners and vendors of Partner (who are natural persons); • Employees or contact persons of Partner's prospects, customers, business partners, and vendors; • Employees, agents, advisors, freelancers of Partner (who are natural persons); • Partner's users authorized by Partner to use Conga Products or Services.
Categories of Personal Data:	The parties may exchange Personal Data for the purpose of the Agreement, which may include Personal Data relating to the following categories of Personal Data • First and last name • Title • Position • Employer • Contact information (company, email, phone, physical business address) • Professional life data • Personal life data • Connection data • Localization data • Contract data
Special Categories of Personal Data:	None.
Frequency of the Transfer:	Regular and repeating for the term of the Agreement, and so long as Partner participates in Conga Partner Program and/or uses or accesses Conga Partner Community website.
Retention Criteria:	Data Importer shall return or delete all transferred Personal Data at the termination of the Agreement, upon Data Exporter's election, as set forth in Section 8 of the DPA.
Subject Matter, Nature, and Duration of Sub-processor Processing:	If Conga acts as a Processor in connection with the subject matter of the Agreement, then Conga's list of Sub-processors is available at https://conga.com/privacy/subprocessors-and-subcontractors, and any related processing performed by those Sub-processors will be as described in this Section B of this Attachment A to the DPA. If Partner acts as a Processor in connection with the subject matter of the Agreement, then Partner's list of Sub-processors shall be provided in accordance with Section 4.9 of the DPA (List of current Sub-Processors and notification of new Sub-Processors).

C. COMPETENT SUPERVISORY AUTHORITY:

The competent supervisory authority shall be as set forth in the relevant sub-part of Section 10 of the DPA.

ATTACHMENT B TO EXHIBIT E

Technical and Organizational Security Measures

Throughout the term of the Agreement, Partner and Conga each shall implement and maintain at least the following security measures:

1. Encryption of Personal Data

All data, including personal data, shall be encrypted in transit using TLS encryption technology. TLS connections are negotiated for at least 256-bit encryption or stronger.

2. Confidentiality, Integrity, Availability and Resilience of Systems and Services

a) Confidentiality and integrity are ensured by taking the following measures:

Access control:

Buildings are protected with appropriate access control systems based on a security classification of the buildings and an appropriately defined access authorization concept. Buildings are secured by access control measures using a card reader system. Depending on the security category, property, buildings or individual areas are secured by additional measures such as special access profiles, separation locks, video surveillanceand security personnel. Access rights for authorized persons are granted individually according to defined criteria. This also applies to external persons.

System access control:

Access to data processing systems is only granted to authenticated users based on a role-based authorization concept using the following measures: Data encryption, individualized password assignment (at least 8 characters, regularly automatic expiration), employee ID cards, password-protected screen savers in case of inactivity, intrusion detection systems and intrusion-prevention systems, regularly updated antivirus and spyware filters in the network and on the individual PCs and mobile devices.

Data access control:

Conga and Partner each will maintain administrative, physical, and technical safeguards sufficient to ensure a reasonable level of security, confidentiality, and integrity for the Personal Data Processed, as described in security documentation made reasonably available by Conga or Partner in connection with this Agreement.

In the instance that Partner uses any of Conga's SaaS solutions, Partner should note that many of Conga's SaaS solutions are hosted on the Salesforce.com platform. Accordingly, certain administration and delegation for user provisioning are the responsibility of the Partner's salesforce.com administrator. Conga employees do not have direct access to the Partner's application environment or data unless they are granted a user login created by the Partner's administrator for the sole purpose of providing technical support services to support the Partner's business needs.

Internally, the provisioning process requires users to change the authentication method upon initial login. Access revocation is conducted upon termination or role change. Role changes for additional access require VP or above approval. Conga uses the least privilege model to ensure access is granted on an approved need to perform job functions. Conga reviews access quarterly. All Conga employees are required to complete security and privacy awareness training as part of onboarding and on an ongoing annual basis and must agree to Conga's privacy and confidentiality requirements.

b) Systems and services constant availability and reliability are ensured by taking the following measures:

Availability and resilience of systems and services are ensured by isolating critical IT and network components, by providing adequate backup and redundancy systems, using power redundancy systems, and regularly testing of systems and services. Test and live systems are kept completely separated.

3. Availability and Access to Personal Data in the Event of an Incident

The availability of and access to personal data in the event of a physical or technical incident shall be restored by taking the following measures: Personal data is stored in RAID systems and integrates redundant systems according to security marking. Systems for uninterruptible power supplies (e. g. UPS, batteries, generators) are

used to secure the power supply in the used data centers. Additionally, databases or data centers are mirrored in different physical locations.

Each party shall maintain a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team shall log and prioritize it according to its severity. Events that directly impact the other party shall be assigned the highest priority. This process shall specify courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff shall be trained in forensics and handling evidence in preparation for an event, including third-party and proprietary tools. To help ensure the swift resolution of security incidents, each party's security team shall be available 24/7 to all employees. If an incident involves the other party's data, the party who suffered the incident will inform the other party and support investigative efforts via its security team.

Each party's Incident Response Plan shall include notifying affected parties and customers of privacy incidents without undue delay and following the terms specified in the Agreement and/or DPA. Each party shall notify affected parties of any actual or reasonably suspected unauthorized access, use, modification, or disclosure of Customer Data by the party or its Sub-processors. Each party shall coordinate communication between its technical support and the affected parties' points of contact on record.

The breach notification would contain a high-level overview of who was impacted, when they were impacted, and the current mitigation status.

4. Control Procedures to ensure the Safety of Processing

A control procedure based on a risk-management-based approach is maintained, taking into account the ISO/IEC 27001 requirements for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure security of processing. This ensures the protection of relevant information, applications (including quality and safety test methods), operating environments (e.g., by network monitoring against harmful effects) and the technical implementation of protection concepts (e.g., by means of vulnerability analyses). By systematically detecting and eliminating weak points, the protective measures are continuously questioned and improved.

5. Monitoring of Vendor Organizations

Each party shall perform an annual review of the security audit reports and certifications relied upon by their vendors having access to Personal Data processed pursuant to the Agreement, as well as any applicable bridge letters, and ensure that such reports and certifications have not lapsed.

6. Personnel Measures

Written work instructions are issued and personnel who have access to personal data are regularly trained to ensure that personal data is only processed in accordance with the law, the Agreement and DPA and associated instructions of the data exporter, including the technical and organizational measures described herein.