

## **DATA PROCESSING ADDENDUM FOR Master Subscription Agreement**

This Data Processing Addendum (“**DPA**”) forms a part of the Master Services Agreement or other similar agreement (the “**Agreement**”) executed by and between Customer (“**Customer**” shall refer to the entity or any Affiliate of the entity bound by the Agreement) and Apttus Corporation, on behalf of itself and its subsidiaries and Affiliates (“**Conga**”). This DPA shall govern the Processing of Personal Data by Conga, and on behalf of Customer, in connection with Conga’s provision of the Services to Customer pursuant to the Agreement. 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 that term is defined below. Where the terms of this Agreement conflict with the terms of an applicable module of the Standard Contractual Clauses, the terms of the applicable module of the Standard Contractual Clauses shall control.

This DPA, along with the associated Attachments, shall be deemed executed, with an effective date as of the date of the Agreement and/or Order Form/Statement of Work to which it relates.

### **1. DEFINITIONS**

Any capitalized term not defined herein shall have the meaning given to that term in the Agreement, or, if not defined in the Agreement, in applicable Data Protection Laws and Regulations.

“**Affiliate**” means any entity (now existing or hereafter formed or acquired), which, directly or through one or more intermediaries, controls, is controlled by, or is under common control with another entity. Ownership of fifty percent (50%) or more of the voting stock, membership interests, partnership interests, or other equity of an entity shall be deemed to be in control over such entity.

“**Authorized Affiliate**” means a Customer’s Affiliate who has not signed an Order Form with Conga but is either permitted to use the Services pursuant to the Agreement between Conga and Customer or is a Data Controller or Data Processor of the Personal Data processed by Conga pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

“**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq.

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

“**Data Processor**” means an entity which Processes Personal Data on behalf of the Data Controller.

“**Data Protection Laws and Regulations**” means all laws and regulations that are applicable to the Processing of Personal Data in connection with the provision of the Services under the Agreement, including but not limited to the CCPA; the GDPR; the other data protection laws and regulations of the European Union (“**EU**”), the European Economic Area (“**EEA**”) and their member states; the data protection laws and regulations of the United Kingdom (“**UK**”); and the data protection laws of Australia, Switzerland, and the United States (“**US**”), each where applicable. Where this DPA intends to refer to the Data Protection Laws and Regulations of a specific jurisdiction, it will designate that jurisdiction as a modifier (for example, “**UK Data Protection Laws and Regulations**,” or “**Australian Data Protection Laws and Regulations**”).

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates.

“**GDPR**” means 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).

“**Personal Data**” means any information relating to (i) an identified or identifiable natural person or (ii) an identified or identifiable legal entity (where protected under applicable Data Protection Laws and Regulations), where such data is submitted to the Services or otherwise Processed in relation to the Services. Where this DPA intends to refer to a subset of Personal Data, the processing of which is regulated by the Data Protection Laws and Regulations of a particular jurisdiction, it will designate that jurisdiction as a modifier (for example, “**EEA Personal Data**,” or “**UK Personal Data**”).

“**Process**”, “**Processes**”, “**Processing**”, or “**Processed**” means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“**Restricted Transfer of Personal Data**” means any transfer of Personal Data from 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 and Regulations.

“**Services**” means the services that Conga performs for Customer pursuant to the Agreement.

“**Standard Contractual Clauses**,” or “**SCCs**,” means the clauses set forth in the European Commission’s decision 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, as set out at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj).

“**Sub-processor**” means any third party appointed by a Data Processor to Process Personal Data on the Data processor’s behalf, in connection with the Data Processor’s provision of services to its Data Controller.

“**UK GDPR**” means the GDPR as implemented or adopted under the laws of the United Kingdom.

### **2. PROCESSING OF PERSONAL DATA**

- 2.1 Roles of the Parties.** As further set forth in the remainder of this Section 2, Conga shall process Personal Data only according to the documented instructions of Customer, and the Parties therefore acknowledge and agree that (i) where Customer is a Data Controller, Conga is a Data Processor, and (ii) where Customer is a Data Processor, Conga is a Sub-processor to Customer. Furthermore, where the CCPA applies to Conga's Processing of Personal Data, the Parties acknowledge and agree that Customer is a Business, as that term is defined within the CCPA and its implementing regulations, and that Conga is Customer's Service Provider, as that term is defined within the CCPA and its implementing regulations.
- 2.2 Customer's Responsibilities.** Customer shall, in Customer's use of the Services, submit or make available Personal Data to Conga for Processing in accordance with the requirements of applicable Data Protection Laws and Regulations. Customer's instructions to Conga for the Processing of Personal Data shall comply with all applicable Data Protection Laws and Regulations. Customer shall have sole responsibility for the initial accuracy, quality, and legality of the Personal Data and of the means by which Customer acquired Personal Data.
- 2.3 Customer's Instructions.** Conga shall Process Personal Data in compliance with applicable Data Protection Laws and Regulations and only according to Customer's documented instructions (including as is necessary to provide the Services to Customer under the Agreement), and Conga shall treat Personal Data as Confidential Information. Customer instructs Conga to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s)/Statement(s) of work, including to provide Customer with the Services; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via e-mail). Conga will notify Customer upon becoming aware of the issue if and when, in Conga's reasonable judgement, Customer's instruction violates Data Protection Laws and Regulations.
- 2.4 Customer's Authorized Affiliates.** The Parties acknowledge and agree that Conga's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:
- 2.4.1** Customer shall remain exclusively responsible for coordinating all communications with Conga directly. Pursuant to Section 2.3, Customer must communicate any additional Processing instructions directly to Conga, including instructions from its Authorized Affiliate.
- 2.4.2** Customer shall be responsible and is solely liable for the Authorized Affiliates' compliance with this DPA and with applicable Data Protection Laws and Regulations, and for all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA. Authorized Affiliate's acts and/or omissions shall be considered the acts and/or omissions of Customer.
- 2.4.3.** Authorized Affiliates shall not bring a claim directly against Conga. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Conga ("**Authorized Affiliate Claim**"): (i) Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to be a party to such claim, Customer must bring such Authorized Affiliate Claim directly against Conga on behalf of such Authorized Affiliate; and (ii) all Authorized Affiliate Claims arising out of or related to this DPA shall be considered claims made by Customer and shall be subject to any limitation of liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

### 3. RIGHTS OF DATA SUBJECTS

- 3.1 Customer's Responsibilities.** Customer maintains full authority and control over all Personal Data for the duration of the Agreement, and Customer acknowledges and agrees that Customer (or Customer's Data Controller(s), where Customer is a Data Processor) is solely responsible for processing and responding to any request, by any Data Subject, to exercise that Data Subject's rights provided for by applicable Data Protection Laws and Regulations, including but not limited to the Data Subject rights provided for by the CCPA and by Chapter III of the GDPR and the UK GDPR. Customer represents, warrants, and agrees that Customer (or Customer's Data Controller(s), where Customer is a Data Processor) shall maintain, throughout the term of the Agreement, (i) a privacy notice, accessible to Data Subjects, that complies with Data Protection Laws and Regulations and that informs Data Subjects, in clear and intelligible language, that they may exercise their rights with respect to any Processing taking place pursuant to the Agreement by contacting Customer (or Customer's Data Controller(s), where Customer is a Data Processor), and not by contacting Conga directly; and (ii) a functioning mechanism for receiving and processing Data Subject requests.
- 3.2 Misdirected Data Subject Requests.** If, despite Customer's compliance with the preceding Section 3.1, Conga receives a request from a Data Subject to exercise that Data Subject's rights provided for by applicable Data Protection Laws and Regulations, Conga will promptly redirect the Data Subject to Customer. Unless legally required to do so, Conga shall not respond to any such Data Subject request without Customer's prior written consent, except to confirm that the request relates to Customer, and Conga shall have no obligation to take any independent action with respect to any Data Subject request beyond redirecting it to Customer.
- 3.3 Assistance with the Execution of Data Subject Requests.** Without contradiction to any of the contents of Sections 3.1 and 3.2, taking into account the nature of the Processing, Conga shall cooperate with and assist Customer in responding to any Data Subject request to exercise that Data Subject's rights provided for by applicable Data Protection Laws and Regulations, but only to the extent Conga is legally permitted to do so, and only to the extent that Customer is not capable of responding to or processing the Data Subject request to correct, amend, block or delete the Personal Data without such assistance from Conga.

### 4. CONGA PERSONNEL AND PRIVACY TEAM CONTACT INFORMATION

- 4.1 **Confidentiality.** Conga shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements or are subject to confidentiality by applicable law. Conga shall ensure that such confidentiality obligations survive the termination of the personnel engagement.
- 4.2 **Limitation of Access.** Conga shall ensure that access to Personal Data by Conga personnel is limited to those personnel who require such access in order for Conga to provide the Services under the Agreement.
- 4.3 **Internal Privacy Office.** Conga's internal privacy office is available at [privacy@conga.com](mailto:privacy@conga.com), and Customer can learn more about Conga's privacy practices, and how to contact Conga's privacy team, at <https://conga.com/privacy>.
- 4.4 **EU Data Protection Representative.** Conga has appointed VeraSafe Ireland Ltd. to serve as Conga's GDPR Article 27 Data Protection Representative within the EEA. VeraSafe Ireland Ltd. is available at:

VeraSafe Ireland Ltd.  
Unit 3D North Point House  
North Point Business Park  
New Mallow Road  
Cork T23AT2P  
Ireland  
Contact Form: <https://verasafe.com/public-resources/contact-data-protection-representative>

- 4.5 **UK Data Protection Representative.** Conga has appointed VeraSafe United Kingdom Ltd. to serve as Conga's GDPR Article 27 Data Protection Representative within the EEA. VeraSafe United Kingdom Ltd. is available at:

VeraSafe United Kingdom Ltd.  
37 Albert Embankment  
London SE1 7TL  
United Kingdom  
Contact Form: <https://verasafe.com/public-resources/contact-data-protection-representative>

- 4.6 **Data Protection Officer.** If and when Conga determines that Conga is required, under applicable Data Protection Laws and Regulations, to appoint a Data Protection Officer, Conga will post that Data Protection Officer's contact details online at <https://www.conga.com/privacy>.

## 5. SECURITY

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 risks, of varying likelihood and severity, for the rights and freedoms of natural persons, Conga shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, as further detailed in Attachment B. Conga regularly monitors compliance with these safeguards. Conga may update these technical and organization measures from time to time, but Conga will not materially decrease the overall security of the Services.

## 6. SECURITY BREACH MANAGEMENT AND NOTIFICATION

Conga maintains security incident management policies and procedures and shall, to the extent permitted by law, without undue delay, and in any event within 48 hours of becoming aware, notify Customer of any actual or reasonably suspected unauthorized access, use, modification, or disclosure of Personal Data in connection with the Processing of that Personal Data by Conga or Conga's Sub-processors (a "**Security Breach**"). Such notice will include all available details required under Data Protection Laws and Regulations to enable Customer to comply with its notification obligations to regulatory authorities or to Data Subjects affected by the Security Breach. Conga shall make all reasonable efforts to identify and take all reasonable steps to remediate the cause of such Security Breach.

## 7. RESTRICTED TRANSFERS OF PERSONAL DATA

- 7.1 **Restricted Transfers of EEA Personal Data.** Where a Restricted Transfer of EEA Personal Data terminates in a jurisdiction that has been the subject of a valid adequacy decision, adopted by the European Commission on the basis of Article 45 of the GDPR, that provides that the receiving jurisdiction ensures an adequate level of protection, no other transfer mechanism shall be necessary. In all other cases, Restricted Transfers of EEA Personal Data shall be conducted pursuant to the Standard Contractual Clauses, or SCCs. Where applicable, this DPA incorporates the SCCs by reference, and the Parties are deemed to have accepted and executed the SCCs in their entirety, including the associated annexes.

- 7.1.1 *Data Controller-to-Data Processor Transfers of EEA Personal Data.* Where Customer, as a Data Controller, transfers or directs the transfer of EEA Personal Data to Conga, as a Data Processor, the Parties agree to implement Module Two of the SCCs, with Customer acting as the "Data Exporter" and Conga as the "Data Importer." The

contents of Annex I of the SCCs are included within Attachment A to this DPA. The contents of Annex II of the SCCs are included within Attachment B. The Parties further agree to the following implementation choices:

- Clause 7: The Parties choose not to include the optional docking clause.
- Clause 9(a): The Parties choose Option 2, “General Written Authorization,” and fifteen (15) days. Customer may view Conga’s current Sub-processor list at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the procedures for designation and notification of new Conga Sub-processors are set forth in more detail in Section 9.4.
- Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
- Clause 13: Where Customer is established in an EU member state, the competent supervisory authority shall be the competent supervisory authority for that member state. Where Customer is not established within an EU member state, but Customer 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 Customer’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 law of the member state where Customer is established or, where such law does not allow for third-party beneficiary rights, by the laws of the Republic of Ireland.
- Clause 18: The Parties select the courts of the Republic of Ireland.

**7.1.2** *Data Processor-to-Sub-processor Transfers of EEA Personal Data.* Where Customer, as a Data Processor, transfers or directs the transfer of EEA Personal Data to Conga, as a Sub-processor, the Parties agree to implement Module Three of the SCCs, with Customer acting as the “Data Exporter” and Conga as the “Data Importer.” The contents of Annex I of the SCCs are included within Attachment A to this DPA. The contents of Annex II of the SCCs are included within Attachment B. The Parties further agree to the following implementation choices:

- Clause 7: The Parties choose not to include the optional docking clause.
- Clause 9(a): The Parties choose Option 2, “General Written Authorization,” and fifteen (15) days. Customer may view Conga’s current Sub-processor list at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the procedures for designation and notification of new Conga Sub-processors are set forth in more detail in Section 9.4.
- Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
- Clause 13: Where Customer is established in an EU member state, the competent supervisory authority shall be the competent supervisory authority for that member state. Where Customer is not established within an EU member state, but Customer 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 Customer’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 law of the member state where Customer is established or, where such law does not allow for third-party beneficiary rights, by the laws of the Republic of Ireland.
- Clause 18: The Parties select the courts of the Republic of Ireland.

**7.2** **Restricted Transfers of Swiss Personal Data.** Where a Restricted Transfer of Swiss Personal Data terminates in a jurisdiction that has been the subject of a valid adequacy decision, adopted by the competent Swiss authorities, that provides that the receiving jurisdiction ensures an adequate level of protection, no other transfer mechanism shall be necessary. In all other cases, Restricted Transfers of Swiss Personal Data shall be conducted pursuant to the SCCs, as they have been adapted for use by the Swiss Federal Data Protection and Information Commissioner (“**FDPIC**”). Where applicable, this DPA incorporates the SCCs by reference, and the Parties are deemed to have accepted and executed the SCCs in their entirety, including the associated annexes.

**7.2.1** *Data Controller-to-Data Processor Transfers of Swiss Personal Data.* Where Customer, as a Data Controller, transfers or directs the transfer of Swiss Personal Data to Conga, as a Data Processor, the Parties agree to implement Module Two of the SCCs, with Customer acting as the “Data Exporter” and Conga as the “Data Importer.” The

contents of Annex I of the SCCs are included within Attachment A to this DPA. The contents of Annex II of the SCCs are included within Attachment B. The Parties further agree to the following implementation choices:

- Clause 7: The Parties choose not to include the optional docking clause.
- Clause 9(a): The Parties choose Option 2, “General Written Authorization,” and fifteen (15) days. Customer may view Conga’s current Sub-processor list at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the procedures for designation and notification of new Conga Sub-processors are set forth in more detail in Section 9.4.
- Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
- Clause 13: Where Customer is established in an EU member state, the competent supervisory authority shall be the competent supervisory authority for that member state. Where Customer is not established within an EU member state, but Customer 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 Customer’s Data Protection Representative is established. In all other cases, the Irish Data Protection Commission will be the competent supervisory authority. However, none of this should be interpreted to preclude Swiss Data Subjects from applying to the FDPIC for relief.
- Clause 17: The clauses shall be governed by the law of the member state where Customer is established or, where such law does not allow for third-party beneficiary rights, by the laws of the Republic of Ireland.
- Clause 18: The Parties select the courts of the Republic of Ireland, with the caveat that the Parties’ selection of forum may not be construed as forbidding Data Subjects in Switzerland from suing for their rights in Switzerland.

**7.2.2** *Data Processor-to-Sub-processor Transfers of Swiss Personal Data.* Where Customer, as a Data Processor, transfers or directs the transfer of Swiss Personal Data to Conga, as a Sub-processor, the Parties agree to implement Module Three of the SCCs, with Customer acting as the “Data Exporter” and Conga as the “Data Importer.” The contents of Annex I of the SCCs are included within Attachment A to this DPA. The contents of Annex II of the SCCs are included within Attachment B. The Parties further agree to the following implementation choices:

- Clause 7: The Parties choose not to include the optional docking clause.
- Clause 9(a): The Parties choose Option 2, “General Written Authorization,” and fifteen (15) days. Customer may view Conga’s current Sub-processor list at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the procedures for designation and notification of new Conga Sub-processors are set forth in more detail in Section 9.4.
- Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
- Clause 13: Where Customer is established in an EU member state, the competent supervisory authority shall be the competent supervisory authority for that member state. Where Customer is not established within an EU member state, but Customer 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 Customer’s Data Protection Representative is established. In all other cases, the Irish Data Protection Commission will be the competent supervisory authority. However, none of this should be interpreted to preclude Swiss Data Subjects from applying to the FDPIC for relief.
- Clause 17: The clauses shall be governed by the law of the member state where Customer is established or, where such law does not allow for third-party beneficiary rights, by the laws of the Republic of Ireland.
- Clause 18: The Parties select the courts of the Republic of Ireland, with the caveat that the Parties’ selection of forum may not be construed as forbidding Data Subjects in Switzerland from suing for their rights in Switzerland.

**7.3 Restricted Transfers of UK Personal Data.** Where a Restricted Transfer of UK Personal Data terminates in a jurisdiction that has been the subject of a valid adequacy decision, adopted by the UK authorities, that provides that the receiving jurisdiction ensures an adequate level of protection, no other transfer mechanism shall be necessary. In all other cases,

Restricted Transfers of UK Personal Data shall be conducted pursuant to the SCCs, as they have been adapted for use by the relevant authorities within the United Kingdom, including the UK Information Commissioner's Office ("UKICO").

**7.3.1** *Data Controller-to-Data Processor Transfers of UK Personal Data.* Where Customer, as a Data Controller, transfers or directs the transfer of UK Personal Data to Conga, as a Data Processor, the Parties agree to implement Module Two of the SCCs, with Customer acting as the "Data Exporter" and Conga as the "Data Importer," 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. In addition, the contents of Annex I of the SCCs are included within Attachment A, and the contents of Annex II of the SCCs are included within Attachment B. The Parties further agree to the following implementation choices:

- Clause 7: The Parties choose not to include the optional docking clause.
- Clause 9(a): The Parties choose Option 2, "General Written Authorization," and fifteen (15) days. Customer may view Conga's current Sub-processor list at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the procedures for designation and notification of new Conga Sub-processors are set forth in more detail in Section 9.4.
- Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
- Clause 13: The UKICO shall be the competent Data Protection 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.
- The Parties further explicitly incorporate by reference any additional modifications and amendments required by the UK Transfer Addendum to make Module Two of the SCCs applicable to Restricted Transfers of UK Personal Data.

**7.3.2** *Data Processor-to-Sub-processor Transfers of UK Personal Data.* Where Customer, as a Data Processor, transfers or directs the transfer of UK Personal Data to Conga, as a Sub-processor, the Parties agree to implement Module Three of the SCCs, with Customer acting as the "Data Exporter" and Conga as the "Data Importer," 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. In addition, the contents of Annex I of the SCCs are included within Attachment A, and the contents of Annex II of the SCCs are included within Attachment B. The Parties further agree to the following implementation choices:

- Clause 7: The Parties choose not to include the optional docking clause.
- Clause 9(a): The Parties choose Option 2, "General Written Authorization," and fifteen (15) days. Customer may view Conga's current Sub-processor list at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the procedures for designation and notification of new Conga Sub-processors are set forth in more detail in Section 9.4.
- Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body.
- Clause 13: The UKICO shall be the competent Data Protection 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.
- The Parties further explicitly incorporate by reference any additional modifications and amendments required by the UK Transfer Addendum to make Module Three of the SCCs applicable to Restricted Transfers of UK Personal Data.

## 8. PROCESSING SUBJECT TO AUSTRALIAN DATA PROTECTION LAWS AND REGULATIONS

Where the Australian Data Protection Laws and Regulations are applicable to Conga's Processing of Personal Data on behalf of Customer in connection with the Agreement, Customer and Conga agree: (i) that the Agreement, including this DPA, serves as a binding contract between Customer and Conga requiring Conga to Process "Personal Information," as that term is defined in Australian Data Protection Laws and Regulations, solely on the documented instructions of Customer, and for no other purpose; (ii) that Conga is contractually obligated to flow through the same obligations to its Sub-processors (*see* Section 9.4); and (iii) that Customer retains effective control over the handling of "Personal Information" by Conga and its Sub-processors. Therefore, Customer and Conga agree that the Processing, by Conga and its Sub-processors, of any Personal Data, or "Personal Information," subject to the Australian Data Protection Laws and Regulations in connection with the provision of Services to Customer pursuant to the Agreement, constitutes a "Use," and not a "Disclosure," by Customer, according to the definitions contained within those same laws and regulations.

## 9. ADDITIONAL TERMS

- 9.1 Subject Matter and Duration of Processing.** The subject matter of the Processing of Personal Data by Conga is the provision of the Services to Customer pursuant to the Agreement, and it shall continue for the term(s) of the Agreement. The details of Processing are set in further in Attachment A.
- 9.2 Nature and Purpose of Processing.** The Processing is related to the provision of SaaS solutions to the Customer, as further detailed within the Agreement, and Conga and its Sub-processors will perform such acts of Processing of Personal Data as are necessary to provide those Services according to Customer's instructions, including but not limited to the transmission, storage, and other Processing of Personal Data submitted to the Services. The details of Processing are set in further in Attachment A.
- 9.3 Supplemental CCPA Data Protection Terms.** In addition to the terms set forth within the body of this DPA, where the CCPA applies to the Processing of Personal Data by Conga and its Sub-processors pursuant to the Agreement, the terms set forth in Attachment C shall apply to such Processing.
- 9.4 Conga's Use of Sub-processors.** Pursuant to this DPA and Clause 9(a) of the Standard Contractual Clauses (if applicable), Customer acknowledges and expressly agrees that: (i) Conga's Affiliates may be retained as Sub-processors; and (ii) Conga and Conga's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.
- 9.4.1 Liability.** Conga shall be liable for the acts and omissions of its Sub-processors to the same extent Conga would be liable if performing the services of each Sub-processor directly.
- 9.4.2 List of Current Sub-processors and Notification of New Sub-processors.** A list of current Sub-processors for the Services is available at <https://conga.com/privacy/subprocessors-and-subcontractors>, and the content of this URL may be updated from time to time. Customer agrees to Conga's use of the listed Sub-processors as of the execution of this DPA. Conga shall provide notification and opportunity to object to any new Sub-processor(s) in accordance with Section 9.4.3 before authorizing any new Sub-processor to Process Personal Data in connection with the provision of the applicable Services. Notification to Customer will be provided to the e-mail address(s) provided in the Order Form for the Service or otherwise to Conga in the purchasing of the Services. Additionally, Customer may sign up for notification at <https://conga.com/privacy/subprocessors-and-subcontractors>. This notification process is Conga's only responsibility for notifying Customer of a new Sub-processor.
- 9.4.3 New Sub-processors.** Conga will, at least 15 days prior to appointing any new Sub-processor, inform Customer of Conga's intent to appoint (including the name and location of such Sub-processor and the activities it will perform) a new Sub-processor by sending an e-mail to Customer and/or by providing Customer with a notification via <https://conga.com/privacy/subprocessors-and-subcontractors>, if Customer has signed up for such notification. Customer may object to Conga's use of a new Sub-processor by notifying Conga promptly in writing within 15 days of receipt of Conga's notice. In the event Customer objects to a new Sub-processor, Conga will use reasonable efforts to make available to Customer a change in the Services or to recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Conga is unable to make available such change within a reasonable period of time, which shall not exceed 30 days, Customer may terminate the applicable Order Form(s)/Statement(s) of Work with respect only to those Services which cannot be provided by Conga without the use of the objected-to new Sub-processor by providing written notice to Conga. Conga will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s)/Statement(s) of Work following the effective date of termination with respect to such terminated Services, without imposing on Customer any penalty for such termination. Conga shall have no penalty or liability for termination under this Section beyond the refund of prepaid

fees and this is Customer sole and exclusive remedy for termination under this Section.

**9.4.4 Sub-processor Agreements.** Conga or a Conga Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement to the extent applicable to the nature of the services provided by such Sub-processor. The Parties agree that the copies of the Sub-processor agreements that must be sent by Conga to Customer pursuant to Data Protection Laws and Regulations may have no commercial information, or clauses unrelated to compliance with the Agreement or DPA removed by Conga beforehand; and, that such copies will be provided by Conga only upon request by Customer.

**9.5 Audits and Certifications.** The Parties agree that the audits described in Clause 8.3, Clause 8.9, and Clause 13 of the Standard Contractual Clauses, where applicable, and otherwise required by applicable Data Protection Laws and Regulations shall be carried out in accordance with the following specifications:

**9.5.1 Certifications and Audit Reports.** Upon Customer’s request, and subject to the confidentiality obligations set forth in the Agreement, Conga shall make available to Customer (or its third-party independent auditor that is not a competitor of Conga) information demonstrating Conga’s compliance with the obligations set forth in this DPA in the form of the certifications, reports, and audit reports for the Services. Examples of potentially relevant certifications and audit reports include: SOC 2; ISO 27001; APEC Cross Border Privacy Rules System; industry codes of conduct or their successor frameworks; and industry standard security questionnaires, such as SIG or CAIQ.

**9.5.2 Additional Audit.** In the event Customer does not find the certifications and audit reports suitable, Conga will make its applicable premises and personnel available to Customer (or its third-party independent auditor that is not a competitor of Conga) for audit upon request and at Customer’s cost. Before the commencement of any such audit, Customer and Conga shall mutually agree upon the scope, timing, and duration of the audit.

**9.5.3 Third-Party Involvement.** In the event Customer conducts an audit through a third-party independent auditor that is not a competitor of Conga, or such a third-party accompanies Customer or participates in such audit, such third-party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Conga’s and Conga’s customers’ confidential and proprietary information. For the avoidance of doubt, government authorities and regulators shall not be required to enter into a non-disclosure agreement.

**9.5.4 Notification of Necessary Changes.** Upon Conga’s request, after conducting an audit, Customer shall notify Conga of the manner in which Conga does not comply with any applicable Data Protection Laws and Regulations, which shall be considered confidential information. If material non-compliance is discovered during Customer’s audit, Conga shall bear the costs, and make any necessary changes to ensure compliance with such obligations, and will, without unreasonable delay, notify Customer when such changes are complete.

**9.6 Return and Deletion of Personal Data.** Where applicable based on the Services, Conga will return and delete Personal Data in accordance with the Agreement, at the election of the Customer, within a reasonable period of time after the conclusion of the Agreement. Customer is responsible for the correction, amendment, blocking or deleting of Personal Data within its control within the Services. However, at the conclusion of the Agreement, Conga will provide reasonable assistance to Customer in the correcting, amendment, blocking or deleting of Personal Data in the Services, where Customer is unable to execute such functions without assistance from Conga.

**9.7 Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the Services and the information available to Conga, and where required to do so by applicable Data Protection Laws and Regulations, Conga will assist Customer in complying with Customer’s obligations regarding data protection impact assessments and prior consultations.

**10. OTHER**

**10.1** This DPA and liability or remedies arising herefrom are subject to any and all limitations on liability and disclaimers of types of damages in the Agreement to the maximum extent permitted by applicable law.


**10.2** This DPA automatically terminates upon termination or expiration of the Agreement.

**10.3** Where any module of the SCCs is applicable, in the event of any conflict or inconsistency between this DPA and/or the Agreement and the SCCs, the terms of the SCCs shall prevail.

**10.4** Notices under the DPA and the Standard Contractual Clauses shall be in accordance with the Agreement.

**Apttus Corporation**

**Customer:**

By:  \_\_\_\_\_

By: \_\_\_\_\_

Name: Stephen Tam

Name: \_\_\_\_\_

Title: Director of Compliance - Information Security

Title: \_\_\_\_\_

Date: 05/13/2022

Date: \_\_\_\_\_



**ATTACHMENT A**  
***Details of Processing***

**A. LIST OF PARTIES:**

**Data Exporter:**

<b>Name:</b>	The Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work and, all Affiliates of Customer.
<b>Address:</b>	Customer's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work
<b>Contact Person:</b>	Customer's telephone number and email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work
<b>Activities Relevant to Transferred Data:</b>	Purchase of Services from Conga.
<b>Role:</b>	Controller or Processor ( <i>see</i> Section 7)

**Data Importer:**

<b>Name:</b>	Apttus Corporation ("Conga")
<b>Address:</b>	13699 Via Varra, Broomfield, CO 80020, USA
<b>Contact:</b>	Security and Compliance, <a href="mailto:privacy@conga.com">privacy@conga.com</a>
<b>Article 27 EU DPR:</b>	<i>See</i> Section 4.4 of the DPA.
<b>Article 27 UK DPR:</b>	<i>See</i> Section 4.5 of the DPA.
<b>Data Protection Officer:</b>	<i>See</i> Section 4.6 of the DPA.
<b>Activities Relevant to Transferred Data:</b>	Conga is a provider of enterprise cloud computing solutions, which Process Personal Data upon the instructions of the Data Exporter in accordance with the terms of the Agreement and DPA.
<b>Role:</b>	Processor or Sub-processor ( <i>see</i> Section 7)

**B. DESCRIPTION OF TRANSFER:**

<b>Subject Matter of the Processing:</b>	The subject matter of the Processing of Personal Data by Conga is the provision of the Services to Data Exporter pursuant to the Agreement.
<b>Nature and Purpose of Processing:</b>	The Processing is related to the provision of SaaS solutions to the Customer, as further detailed within the Agreement, and Conga and its Sub-processors will perform such acts of Processing of Personal Data as are necessary to provide those Services according to Data Exporter's instructions, including but not limited to the transmission, storage, and other Processing of Personal Data submitted to the Services.
<b>Duration of Processing:</b>	Conga will process Personal Data on behalf of the Data Exporter until Data Exporter ceases use of the Services.
<b>Categories of Data Subjects:</b>	Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled solely by the Data Exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects: <ul style="list-style-type: none"> <li>• Prospects, customers, business partners and vendors of Data Exporter (who are natural persons)</li> <li>• Employees or contact persons of Data Exporter's prospects, customers, business partners and vendors</li> <li>• Employees, agents, advisors, freelancers of Data Exporter (who are natural persons)</li> </ul>

	<ul style="list-style-type: none"> <li>Data Exporter’s users authorized by Data Exporter to use the Services</li> </ul>
<b>Categories of Personal Data:</b>	<p>Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled solely by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:</p> <ul style="list-style-type: none"> <li>First and last name</li> <li>Title</li> <li>Position</li> <li>Employer</li> <li>Contact information (company, email, phone, physical business address)</li> <li>ID data</li> <li>Professional life data</li> <li>Personal life data</li> <li>Connection data</li> <li>Localization data</li> <li>Contract data</li> </ul>
<b>Special Categories of Personal Data:</b>	<p>Data Exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which is, for the sake of clarity, Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life.</p>
<b>Frequency of the Transfer:</b>	<p>Regular and repeating for as long as Data Exporter uses the Services.</p>
<b>Retention Criteria:</b>	<p>Generally, retention of Personal Data should not be required. In case Personal Data should be retained, any retention period will be limited to the duration absolutely necessary to perform the Services pursuant to the Agreement.</p>
<b>Subject Matter, Nature, and Duration of Sub-processor Processing:</b>	<p>Any transfer to Sub-processors will be in order to perform the Services pursuant to the Agreement. Data processed is stored on servers of Salesforce, Amazon Web Services, and ancillary functions process application data as described in the security documentation applicable to the specific Services licensed by Customer, and accessible via <a href="https://conga.com/security-data-sheets">https://conga.com/security-data-sheets</a> or otherwise made reasonably available by Conga.</p>

**C. COMPETENT SUPERVISORY AUTHORITY:**

The competent supervisory authority shall be as set forth in the relevant sub-part of Section 7 of the DPA.

## ATTACHMENT B

### *Technical and Organizational Security Measures*

#### **1. Encryption of Personal Data**

All data, including personal data, is 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 surveillance and 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 will maintain administrative, physical, and technical safeguards for the protection, security, confidentiality and integrity of Personal Data Processed by the Services, as described in the security documentation applicable to the specific Services licensed by Customer, and accessible via <https://conga.com/security-data-sheets> or otherwise made reasonably available by Conga. 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 customer's salesforce.com administrator. Conga employees do not have direct access to the client's application environment or data unless they are granted a user login created by the client's administrator for the sole purpose of providing technical support services to support the client'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.

Conga has 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 logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff is 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, the Conga security team is available 24/7 to all employees. If an incident involves customer data, Conga will inform the customer and support investigative efforts via our security team.

Conga's Incident Response Plan includes notifying affected customers of privacy incidents without undue delay and following the terms specified in the Agreement and/or DPA. Conga would notify affected customers of any actual or reasonably suspected unauthorized access, use, modification, or disclosure of Customer Data by Conga or its Sub-processors. We will coordinate communication between the technical support and the points of contact Conga has 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 the Subservice Organization**

Conga management performs an annual review of the Salesforce System and Organization Controls (SOC) 1, Type 2 report that is issued on an annual basis, as well as any applicable bridge letters. Management’s review consists of ensuring the complementary user entity controls are met and analyzing any findings for impact on the organization.

**6. Application and Development Maintenance**

Conga has a well-defined System Development Life Cycle (SDLC) methodology that governs the application development and change management process. Conga enforces that the SDLC policies and procedures are reviewed annually and are updated on an as-needed basis to reflect changes in the operating environment.

**7. 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.

---

## ATTACHMENT C

### *Supplemental CCPA Data Protection Terms*

Words and phrases defined in the CCPA shall have the same meaning in this Attachment and all other terms shall have the meaning assigned by the DPA or Agreement, each as applicable. In the event of a conflict between the terms of this Attachment and the Agreement, this Attachment will control, but all other terms in the Agreement will otherwise remain in full force.

#### **1. The following definitions and rules of interpretation apply in this Attachment:**

- (a) “CCPA” means the California Consumer Privacy Act of 2018, (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations provided by the California Attorney General all of which as may be amended from time to time.
- (b) “Contracted Business Purposes” means the Services and as otherwise described in the Agreement for which the Conga receives or accesses personal information from Customer.

#### **2. Conga's CCPA Obligations:**

- (a) Conga will only collect, use, retain, or disclose personal information for the Contracted Business Purposes for which Customer provides or permits personal information access.
- (b) Conga will not collect, use, retain, disclose, sell, or otherwise make personal information available in a way that does not comply with the CCPA. If a law requires Conga to disclose personal information for a purpose unrelated to the Contracted Business Purpose, Conga must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless applicable law prohibits such notice.
- (c) To the extent commercially reasonable, Conga will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible operational purpose.
- (d) Conga must promptly comply with any Customer request or instruction requiring the Conga to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing. If Customer is able to amend, transfer, or delete the personal information itself and chooses Conga's assistance, Customer agrees to pay reasonable fees for such assistance at a rate mutually agreed in advance between the Parties.
- (e) If the Contracted Business Purposes require the collection of personal information from individuals on the Customer's behalf, Conga will always provide a CCPA-compliant notice addressing use and collection methods.
- (f) If the CCPA permits, Conga may aggregate, deidentify, or anonymize personal information, so it no longer meets the personal information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes. Conga will not attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data.

#### **3. Assistance with CCPA Obligations:**

- (a) Conga will reasonably cooperate and assist Customer in responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of Conga's processing and the information available Conga.
- (b) A party must notify the other party promptly if it receives any complaint, notice, or communication that directly or indirectly relates to either party's compliance with the CCPA. Specifically, Conga must notify the Customer within five (5) working days if it receives a verifiable consumer request under the CCPA.

#### **4. Subcontracting:**

- (a) Conga may use subcontractors to provide the Contracted Business Services. Conga cannot make any disclosures to the subcontractor that the CCPA would treat as a sale, and Conga shall ensure appropriate terms no less protective than those in this Attachment are entered into between Conga and the subcontractor.
- (b) Conga remains fully liable for each subcontractor's performance to the same extent if Conga were performing itself.
- (c) Upon the Customer's written request, Conga will provide Customer with information and reports demonstrating Conga's compliance with the obligations in this Attachment.

#### **5. Certifications:**

- (a) Both Parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing personal information.
- (b) Conga certifies that it understands this Attachment's and the CCPA's restrictions and prohibitions on selling personal information and retaining, using, or disclosing personal information outside of the Parties' business relationship, and Conga will comply with them.