DATA PROCESSING ADDENDUM FOR
Master Services Agreement

This Data Processing Addendum ("**DPA**") forms part of the Master Services Agreement, or other similar agreement pertaining to the Processing of Customer Personal Data (the "**Agreement**") between Customer ("**Customer**" shall mean the entity or entity's Affiliates bound by the Agreement) and Apttus Corporation, on behalf of itself and its subsidiaries and affiliates, including AppExtremes, LLC, ("**Conga**"). This DPA reflects the Parties' agreement with regards to the applicable Data Protection Laws and Regulations.

HOW THIS DPA APPLIES

The terms of this DPA only apply to Customer and Conga as follows:

A. Sections 1 through 8, Attachment 1, Annex I, and Annex II apply when Data Protection Laws and Regulations apply to the Agreement.
B. When only the CCPA applies to the Agreement, then only Section 8 and Attachment 2 apply.
C. The entire DPA along with all appendices and attachments apply when Data Protection Laws and Regulations and the CCPA apply to the Agreement.

1. DEFINITIONS

Any capitalized terms not defined herein shall have the meaning given to that term in the Agreement, CCPA, or 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 Customer 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 the entity which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws and Regulations" means all laws and regulations, applicable to the Processing of Personal Data with the Services under the Agreement, including CCPA, EU General Data Protection Regulation ("**GDPR**"), laws and regulations of the European Union, the European Economic Area ("**EEA**") and their member states, Switzerland, the United States, and the United Kingdom.

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means any information (i) of an identified or identifiable person and, (ii) of 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.

"Process", Processes", "Processing", Processed" means any operation or set of operations which is 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.

"Services" means any and all services that Conga performs under the Agreement.

"Standard Contractual Clauses" means, when applicable, the agreement executed by and between Customer and Conga and attached hereto as Attachment 1 pursuant to 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 found at ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

"Subprocessor" means any third party appointed by or on behalf of Conga to Process Personal Data in connection with the Services.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller and Conga is a Data Processor.

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 the Data Protection Laws and Regulations, and Customer's instructions to Conga for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the initial accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 Customer's Instructions. Conga shall only Process Personal Data on behalf of and in accordance with Data Protection Laws and Regulations, Customer's instructions (including as is necessary to provide the Services to Customer under the Agreement), and 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 you 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 and if in Conga's reasonable judgement that Customer's instruction violates Data Protection Laws and Regulations.

2.4 Customer 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 exclusively remain 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 Affiliates;

2.4.2 Customer shall be responsible and is solely liable for the Authorized Affiliates' compliance with this DPA and 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; and

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 Correction, Blocking, and Deletion. To the extent Customer, in Customer's use of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws and Regulations, Conga shall assist Customer in facilitating such actions to the extent Conga is legally permitted to do so.

3.2 Data Subject Requests. Conga shall, to the extent legally permitted, promptly notify Customer if Conga receives a request from a Data Subject for access to, correction, amendment or deletion of that Data Subject's Personal Data. If legally permitted, 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. Conga shall cooperate and assist in responding to a Data Subject's request for access to their Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through use of the Services.

4. CONGA PERSONNEL

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 Conga's access to Personal Data is limited to those personnel who require such access to perform under the Agreement.

4.3 EU Representative/UK Representative/Data Protection Officer. If required by Data Protection Laws and Regulations, Conga will appoint an EU Representative, UK Representative, and/or Data Protection Officer which may be contacted at privacy@conga.com. Further details can be found at https://conga.com/privacy. In the event Data Protection Laws and Regulations change as to the requirements of an EU Representative, UK Representative, and/or Data Protection Officer,the aforementioned URL will be updated, and the designated EU Representative, UK Representative, and/or Data Protection Officer will be as listed there.

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 risk 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 Annex II. Conga regularly monitors compliance with these safeguards. Conga may update these technical and organization measures from time to time, but 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, by Conga or its Subprocessors (a "**Security Breach**"). Such notice will include all available details required under Data Protection Laws and Regulations for Customer to comply with its own notification oblitations to regulatory authorities or individuals 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. ADDITIONAL TERMS

7.1 Application of Standard Contractual Clauses. The Standard Contractual Clauses in Attachment 1 and the additional terms in Section 7 will apply to the Processing of Personal Data by Conga in the course of providing Services as follows:

7.1.1 Notwithstanding anything to the contrary in this DPA, the Standard Contractual Clauses apply only to Personal Data that is transferred from the EEA, Switzerland, and/or the United Kingdom to outside the EEA, Switzerland, and/or the United Kingdom, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR), and (ii) not covered by a suitable framework (e.g. Binding Corporate Rules for Processors, EU-US and Swiss-US Privacy Shield, etc.) recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

7.1.2 Subject to Section 7.1.1, the Standard Contractual Clauses apply to (i) the legal entity that has executed the Agreement and is the Data Exporter, and (ii) all Affiliates (as defined in the Agreement) of Customer established in the EEA, Switzerland or the United Kingdom that have licensed the Services. For the purpose of the Standard Contractual Clauses and this Section 7, the aforementioned entities shall be deemed "Data Exporters".

7.2 Objective and Duration. The objective of Processing of Personal Data by Conga is the provision of the Services pursuant to the Agreement for the term(s) of the Agreement.

7.3 Subprocessors. Pursuant to this DPA and Clause 9(a) of the Standard Contractual Clauses (if applicable), Customer acknowledges and expressly agrees that: (a) Conga's Affiliates may be retained as Subprocessors; and (b) Conga and Conga's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services.

7.3.1 Liability. Conga shall be liable for the acts and omissions of its Subprocessors to the same extent Conga would be liable if performing the services of each Subprocessor directly.

7.3.2 List of Current Subprocessors and Notification of New Subprocessors. A list of current Subprocessors for the Services is available at https://conga.com/privacy/subprocessors, the content of this URL may be updated from time to time and Customer agrees to Conga's use of the listed Subprocessors as of the execution of this DPA. Conga shall provide notification and opportunity to object to any new Subprocessors in accordance with Section 7.3.3 before authorizing any new Subprocessor 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. This notification process is Conga's only responsibility for notifying Customer of a new Subprocessor.

7.3.3 New Subprocessors. Conga will, at least 15 days prior to appointing any new Subprocessor, inform Customer of Conga's intent to appointment (including the name and location of such Subprocessor and the activities it will perform) a new Subprocessor by sending an e-mail to Customer and/or a notification via https://conga.com/privacy/subprocessors, if Customer has signed up for such notification. Customer may object to Conga's use of a new Subprocessor by notifying Conga promptly in writing within 15 days of receipt of Conga's notice. In the event Customer objects to a new Subprocessor, Conga will use reasonable efforts to make available to Customer a change in the Services or 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 Subprocessor 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 Subprocessor 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.

7.3.4 Subprocessor Agreements. Conga or a Conga Affiliate has entered into a written agreement with each Subprocessor 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 Subprocessor. The Parties agree that the copies of the Subprocessor 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.

7.4 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 and otherwise required by applicable Data Protection Laws and Regulations shall be carried out in accordance with the following specifications:

7.4.1 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; industry standard security questionnaires, such as SIG or CAIQ.

7.4.2 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 auditror

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.

7.4.3 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.

7.4.4 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.

7.5 Return and Deletion of Personal Data. Where applicable based on the Services, Conga will return and delete Personal Data in accordance with the Agreement. Customer is responsible for the correction, amendment, blocking or deleting of Personal Data within its control within the Services. Conga will provide reasonable assistance to Customer in the correcting, amendment, blocking or deleting of Personal Data in the Services.

7.6 Privacy Impact Assessment and Prior Consultation. Taking into account the nature of the Services and the information available to Conga, Conga will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation pursuant to the GDPR.

8. OTHER

8.1 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.

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

8.3 Subject to applicability in accordance with Section 7.1, in the event of any conflict or inconsistency between this DPA and/or the Agreement, and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail.

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

ATTACHMENT 1 TO THE DPA
Standard Contractual Clauses (MODULE TWO: Transfer controller to processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

---

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out

regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

([3]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or

Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the EU Member State in which the data exporter has its seat. If the Agreement is not governed by an EU Member State law, these Clauses shall be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I
TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):

1. Name: The Customer identified in the Agreement and/or Order Form(s)/Statement(s) of work and, all Affiliates of Customer established within the European Economic Area (EEA), the United Kingdom and/or Switzerland

   Address: Customer's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of work

   Contact person's name, position and contact details: Customer's telephone number and email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of work

   Activities relevant to the data transferred under these Clauses: Purchase of Services from the data importer

   Signature and date: This Annex 1 shall be deemed signed with and effective as of the date of the Agreement and/or Order Form/Statement of work of which it forms part.

   Role (controller/processor): Controller

Data importer(s):

1. Name: **Apttus Corporation**, for itself and its Affiliates, located outside EU/EEA, the United Kingdom, and/or Switzerland

   Address: 13699 Via Varra, Broomfield, CO 80020, USA

   Contact person's name, position and contact details: Kennith Asher, Senior Director of Security and Compliance, privacy@conga.com

   Activities relevant to the data transferred under these Clauses: Apttus Corporation is a provider of enterprise cloud computing solutions, which Process Personal Data upon the instruction of the data exporter in accordance with the terms of the Agreement and the DPA.

   Signature and date: This Annex 1 shall be deemed signed with and effective as of the date of the Agreement and/or Order Form/Statement of work of which it forms part.

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

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:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's users authorized by data exporter to use the Services

Categories of personal data transferred:

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:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- professional life data
- personal life data
- connection data
- localization data
- contract data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

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.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): One-off/sporadically

Nature of the processing: The processing required to provide the requested Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing: The performance of the Services pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Generally, retention of personal data should not be required. In case personal data should exceptionally be retained, any retention period will be limited to the duration absolutely necessary to perform the Services pursuant to the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

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 https://conga.com/security-data-sheets or otherwise made reasonably available by Conga

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The competent supervisory authority of the EU Member State in which the data exporter has its seat.

ANNEX II
TO THE STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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 Subprocessors. 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.

5. 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 2 TO THE DPA

Words and phrases defined in the CCPA shall have the same meaning in this Appendix and all other terms shall have the meaning in the DPA or Agreement. In the event of a conflict between the terms of this Appendix and the Agreement, this Appendix 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 Appendix:

(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 Appendix 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 Appendix.

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 Appendix'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.