GO-CORT, INC. END USER LICENSE AGREEMENT - DATA PROCESSING ADDENDUM

1. Acceptance.

1.1. This Go-Cort, Inc. End User License Agreement - Data Processing Addendum (this "Addendum") constitutes a binding agreement by and between Go-Cort, Inc., an Oregon corporation dba Apptoto ("Apptoto") and you, the customer ("Customer"). This Addendum is incorporated into and made part of the Go-Cort, Inc. End User License Agreement (the "EULA") previously or contemporaneously entered into by Customer and governs the processing of personal data that Customer uploads or otherwise provides to Go-Cort, Inc. If you are entering into this Agreement on behalf of an entity or organization, you are representing and warranting that you have the authority to bind the Customer and you are agreeing to these terms on behalf of yourself and the Customer. Collectively, this Addendum and the EULA are referred to in this Addendum as the "Go-Cort, Inc. Agreement." In the event of any conflict or inconsistency between any of the terms of this Addendum and the terms of the EULA, the terms of this Addendum will prevail as it relates to the subject matter herein. Except as specifically amended by this Addendum, the EULA and any other applicable agreements between Customer and Apptoto remain unchanged and in full force and effect.

2. Definitions.

2.1. "Go-Cort, Inc. Services" means any services or Software (as defined in the EULA) that Go-Cort, Inc. provides to Customer in connection with the Go-Cort, Inc. Agreement.

2.2. "Controller" means the natural or legal person, public authority, agency, or other body, which, alone or jointly with others, determines the purposes and means of the processing of Customer Personal Data.

2.3. "Customer Personal Data" means Personal Data that Customer uploads, integrates, or otherwise provides to Go-Cort, Inc. in connection with Apptoto Services.

2.4. "General Data Protection Regulation" or "GDPR" means the European Union Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC, and includes any applicable subsequent legislation and regulations implementing the GDPR.

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

2.6. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored, or otherwise processed.

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

2.8. “Processor” means a natural or legal person, public authority, agency, or other body, which processes Customer Personal Data on behalf of the Controller.

2.9. “Subprocessor” means any entity that provides processing services to Go-Cort, Inc. in furtherance of Go-Cort, Inc.’s processing on behalf of Customer.

2.10. “Supervisory Authority” means an independent public authority established by a European Union member state pursuant to Article 51 of the General Data Protection Regulation.

3. Data Processing.

3.1. Roles of the Parties. Customer is the Controller and Go-Cort, Inc. is the Processor of Customer Personal Data. Customer appoints Go-Cort, Inc. as Processor to process Customer Personal Data and to engage Subprocessors in accordance with this Addendum.

3.2. Scope of Processing. Go-Cort, Inc. will process Customer Personal Data as necessary to provide Go-Cort, Inc. Services, and as further instructed by Customer in writing in connection with the Go-Cort, Inc. Agreement.

3.3. Duration of Processing. Subject to Section 8 of this Addendum, Go-Cort, Inc. will process Customer Personal Data for the duration of the Go-Cort, Inc. Agreement, unless otherwise agreed in writing.

3.4. Categories of Data Subjects. Customer may submit Personal Data to Go-Cort, Inc., the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

3.4.1. Prospective clients, clients, business partners, and vendors of Customer (who are natural persons);

3.4.2. Employees, agents, family members, and contact persons of Customer’s prospective clients, clients, business partners, and vendors;

3.4.3. Employees, agents, advisors, and freelancers of Customer (who are natural persons); or

3.4.4. Users authorized by Customer to use Go-Cort, Inc. Services.

3.5. Categories of Customer Personal Data. Customer may submit Personal Data to Go-Cort, Inc., the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

3.5.1. First, middle, and last name and nicknames;

3.5.2. Title;

3.5.3. Email address;

3.5.4. Phone number;

3.5.5. Other contact information;

3.5.6. Appointment information (event title, location, notes, time)

3.5.7. IP address; or

3.5.8. Personal life data (including additional notes added by user).

3.6. Compliance with Law. Customer is solely responsible for the lawfulness of the Processing of Customer Personal Data and the lawfulness of the means by which Customer acquires Customer Personal Data, including, without limitation, the scope and adequacy of consent from Data Subjects. Customer agrees that its use of Go-Cort, Inc. Services for the Processing of Customer Personal Data will comply with applicable law, including, without limitation, the GDPR.

3.7. Compliance with Customer Instructions. Go-Cort, Inc. will process Customer Personal Data on behalf of Customer and in accordance with Customer’s instructions for the purposes described

in the Go-Cort, Inc. Agreement and for the purposes of and as initiated by Customer's users of the Go-Cort, Inc. Services. If Go-Cort, Inc. believes that an instruction from Customer violates applicable law, including, without limitation, the GDPR, Go-Cort, Inc. will notify Customer without undue delay and may suspend performance until Customer has modified or confirmed the lawfulness of the instruction in writing.

3.8. Other Controllers. Customer will serve as a single point of contact for Go-Cort, Inc. with respect to Customer Personal Data. To the extent that other Controllers may have any rights as joint Controllers with Customer with respect to Customer Personal Data, Customer agrees to exercise all such rights on their behalf and to obtain all necessary approvals and consents from the other Controllers. Go-Cort, Inc. will have no obligation to inform or notify such other Controllers when Go-Cort, Inc. has provided such information or notice to Customer.

4. Security Measures and Breach Response.

4.1. Security Measures. Go-Cort, Inc. will implement and maintain technical and organizational measures as set forth in Exhibit 1 ("Security Measures") to ensure a level of security appropriate to the risk for Go-Cort, Inc.'s scope of responsibility. These measures are subject to technical progress and further development. Go-Cort, Inc. reserves the right to modify these measures from time to time, so long as the functionality and security of Go-Cort, Inc. Services materially comply with applicable law.

4.2. Notice to Customer of Personal Data Breach. Go-Cort, Inc. will notify Customer without undue delay after becoming aware of a Personal Data Breach with respect to Go-Cort, Inc. Services.

4.3. Assistance to Customer. Go-Cort, Inc. will reasonably assist Customer, at Customer's expense, in ensuring compliance with Customer's obligations relating to the security of Processing, the notification of a Personal Data Breach, and the conduct of a data protection impact assessment, taking into account the information available to Go-Cort, Inc.

4.4. Personal Data Breach Response. Go-Cort, Inc. will promptly investigate a Personal Data Breach if it occurred on Go-Cort, Inc. infrastructure or in another area for which Go-Cort, Inc. is responsible. Go-Cort, Inc. will make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as Go-Cort, Inc. deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach to the extent the remediation is within Go-Cort, Inc.'s reasonable control. The obligations in this Section 4.4 will not apply to incidents that are caused by Customer or Customer's users.

5. Data Subject Rights and Requests.

5.1. Data Subject Requests. Go-Cort, Inc. will, to the extent legally permitted, promptly notify Customer if Go-Cort, Inc. receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to automated individual decision making ("Data Subject Request"). Customer is solely responsible for responding to a Data Subject Request. To the extent practicable by appropriate technical and organizational measures, and to the extent Go-Cort, Inc. is legally permitted to do so, Go-Cort, Inc.will use commercially reasonable efforts to assist Customer, at Customer's expense, in complying with Customer's obligation to respond to a Data Subject Request in accordance with applicable law, including, without limitation, the GDPR.

6. Third Party Requests; Confidentiality.

6.1. No Unauthorized Disclosure. Except in accordance with the Go-Cort, Inc. Agreement and as permitted by applicable law, Go-Cort, Inc. will not disclose Customer Personal Data to any third party. If a Supervisory Authority demands access to Customer Personal Data, Go-Cort, Inc. will

notify Customer prior to disclosure, unless prohibited by applicable law, in which case no prior notice is required.

6.2. Restrictions on Use. Go-Cort, Inc. shall treat all Customer Personal Data as confidential and shall process Customer Personal Data in accordance with the Go-Cort, Inc. Agreement and for no other purpose unless required by applicable law.

7. Audit.

7.1. Cooperation. Go-Cort, Inc. will allow for and contribute to audits, including inspections, conducted by Customer or another auditor designated by Customer of Go-Cort, Inc.'s Processing of Customer Personal Data, subject to the following procedures:

7.1.1. On Customer's written request, Go-Cort, Inc. will provide Customer or its designated auditor with the most recent certifications and/or summary audit report(s), which Go-Cort, Inc. has procured to regularly test, assess, and evaluate the effectiveness of its Security Measures.

7.1.2. Go-Cort, Inc. will reasonably cooperate with Customer by providing available additional information concerning its Security Measures, to help Customer better understand such Security Measures.

7.1.3. If Customer needs further information to comply with its own or another Controller's audit obligations or a competent Supervisory Authority's request, Customer will inform Go-Cort, Inc. in writing to enable Go-Cort, Inc. to provide such information or to grant Customer access to it.

7.1.4. To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable law, only legally mandated entities (such as a governmental regulatory agency having oversight of Customer's operations), Customer, or its designated auditor may conduct an onsite visit of the facilities used to perform Processing pursuant to the Agreement, during normal business hours and only in a manner that causes minimal disruption to Go-Cort, Inc.'s business, subject to coordinating the timing of such visit and in accordance with any audit procedures reasonably necessary in order to reduce any risk to Go-Cort, Inc.'s other customers.

7.2. Costs. Each party will bear its own costs of performing its obligations under Sections 7.1.1 and 7.1.2. Any further assistance with be at Customer's sole expense unless otherwise agreed to in writing by Go-Cort, Inc.

8. Return or Deletion of Customer Personal Data.

8.1. Deletion On Termination. On expiration or earlier termination of the Agreement, Go-Cort, Inc. will either delete or return Customer Personal Data in its possession or control, unless otherwise required or permitted by applicable law.

9. Subprocessors.

9.1. Subprocessing Permitted. Customer authorizes Go-Cort, Inc. to engage subcontractors to process Customer Personal Data. A list of current Subprocessors is set out in attached Exhibit 2. Go-Cort, Inc. will give Customer not less than 10 days' advance written notice of any changes to Go-Cort, Inc.'s Subprocessors. Within ten (10) days after Go-Cort, Inc.'s notification of the intended change, Customer can object to the addition of a Subprocessor on the basis that such addition would cause Customer to violate applicable law. Customer's objection will be in writing and include Customer's specific reasons for its objection, including the applicable legal requirements, and options to mitigate, if any. If Customer does not object within such period, the respective Subprocessor may be authorized to process Customer Personal Data. Go-Cort, Inc. will impose substantially similar data protection obligations as set out in this Addendum on any approved Subprocessor prior to the Subprocessor Processing any Customer Personal Data.

9.2. Notice of Objection. If Customer legitimately objects to the addition of a Subprocessor and Go-Cort, Inc. cannot reasonably accommodate Customer's objection, Go-Cort, Inc. will notify Customer. Customer may terminate the Go-Cort, Inc. Agreement with respect only to those Go-Cort, Inc. Services that cannot be provided by Go-Cort, Inc. without the use of the objectionable Subprocessor by providing Go-Cort, Inc. with a written notice within thirty (30) days of Go-Cort Inc.'s notice. Go-Cort, Inc. will refund a prorated portion of any prepaid charges for the period after such termination date, without penalty for such termination.

10. Transborder Data Processing.

10.1. Standard Contractual Clauses. By agreeing to this Addendum, Customer is entering into the EU Standard Contractual Clauses as referred to in attached Exhibit 3, with the Subprocessors established outside either the European Economic Area or countries considered by the European Commission to have adequate protection ("Data Importers").

10.2. Other Controllers. Customer agrees on behalf of any other Controller of Customer Personal Data, or if unable to agree, will procure agreement of such Controller, to be an additional data exporter with respect to the EU Standard Contractual Clauses concluded between Go-Cort, Inc. and Customer. Go-Cort, Inc. accepts the agreement of such other Controller. Customer agrees and, if applicable, procures the agreement of any other Controller that the EU Standard Contractual Clauses, including any claims arising from them, are subject to the terms set forth in the Go-Cort, Inc.Agreement, including, without limitation, the exclusions and limitations of liability. In case of conflict, the EU Standard Contractual Clauses will prevail.

11. Indemnity; Limitation of Liability.

11.1. Indemnity. In addition to and not in lieu of existing indemnification obligations in the EULA, Customer agrees to indemnify, defend, and hold Go-Cort, Inc. harmless for, from, and against, any and all costs, charges, damages, expenses (including attorney's fees), and losses arising from or related to Customer's breach of this Addendum, including, without limitation, non-compliance with the GDPR.

11.2. Limitation of Liability. Each party's liability arising out of or related to this Addendum, whether in contract, tort, or under any other theory of liability, is subject to any and all limitations of liability in the EULA.

12. Last Updated: January 2021.

EXHIBIT 1

SECURITY MEASURES

1. **Access**
    a. Access to private information about data subjects is limited to employees of Go-Cort, Inc. Those employees include support and operations personnel.
    b. Support personnel may see the information but only to provide support requested by Customer. All access is logged and monitored. Our CEO is notified every time support personnel access Customer Personal Data. Two-factor authentication is required for use by support personnel.
    c. Operations personnel have access to the infrastructure used to run Go-Cort, Inc. (including servers and databases). Operations personnel may see the information within a Customer's account through server consoles, but only while performing operations required to support Go-Cort, Inc.'s processing.
    d. All support and operations personnel undergo extensive background checks before being hired.

2. **Encryption**
    a. All data is strongly encrypted (minimum key length is 256 bits) in transit between:
        i. Customer and Go-Cort, Inc. (through website portal and API)
        ii. Go-Cort, Inc. and Subprocessors (through API)
    b. All data is strongly encrypted at rest on disk.

3. **Security (System, Physical, Environmental)**
    a. All servers under control of Go-Cort, Inc. run virus detection software.
    b. All workstations under control of Go-Cort, Inc. run virus detection software.
    c. All personnel are required to leverage password managers and 2FA when available.
    d. All servers and databases are only accessible to operations personnel through VPN and Bastion gateways.

4. **Periodic Assessments**
    a. Periodic virus detection software assessment
    b. Periodic assessment of Acceptable Use Policy by personnel (see apptoto.com for downloadable Security Policy PDFs)
    c. Monthly web application security assessments through
        i. OWASP ZAP
        ii. Tinfoil Security Scanner

5. **Incident Response**
    a. See apptoto.com for downloadable Security Policy PDFs

EXHIBIT 2

SUBPROCESSORS

- Amazon Web Services
- Armor.com (for Healthcare clients)
- Twilio
- Sendgrid
- Mailgun
- Clicksend

EXHIBIT 3

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:

Address:

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organization:

(the data **exporter**)

And

Name of the data importing organization: Go-Cort, Inc.

Address: 61149 South Highway 97 #505, Bend, OR 97701

Tel.: 888-318-3765; e-mail: support@apptoto.com

Other information needed to identify the organization:

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 - Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of

personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1, which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be

transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects On request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

  (ii) any accidental or unauthorised access; and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject On request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 - Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 - Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed On the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that On request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature_____

On behalf of the data importer:

Name (written out in full): Frank Cort

Position: President

Address: 61149 South Highway 97 #505, Bend, OR 97701

Other information necessary in order for the contract to be binding (if any):

Signature_____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:

Data importer
The data importer is:
Go-Cort, Inc. (DBA Apptoto)

Data subjects
The personal data transferred concern the following categories of data subjects:

- Prospective clients, clients, business partners, and vendors of Customer (who are natural persons);
- Employees, agents, family members, and contact persons of Customer's prospective clients, clients, business partners, and vendors;
- Employees, agents, advisors, and freelancers of Customer (who are natural persons); or
- Users authorized by Customer to use Apptoto Services.

Categories of data
The personal data transferred concern the following categories of data:

- First, middle, and last name and nicknames;
- Title;
- Email address;
- Phone number;
- Other contact information;
- Appointment information (event title, location, notes, time);
- IP address; or
- Personal life data (including additional notes added by user).

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

- Health data.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

- Processing of Appointment Data in order to send automated messages before, during, and after appointments.
- Also processing of Appointment Data to facilitate scheduling of new appointments.

DATA EXPORTER

Name:

Authorized Signature _____

DATA IMPORTER

Name:

Authorized Signature _____

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Access**
    a. Access to private information about data subjects is limited to employees of Go-Cort, Inc. (DBA Apptoto) Those employees include support and operations personnel.
    b. Support personnel may see the information but only to provide support requested by Customer. All access is logged and monitored. Our CEO and Chief Privacy Officer is notified every time support personnel access Customer Personal Data. Two-factor authentication is required for use by support personnel.
    c. Operations personnel have access to the infrastructure used to run Apptoto (including servers and databases). Operations personnel may see the information within a Customer's account through server consoles, but only while performing operations required to support Apptoto's processing.
    d. All support and operations personnel undergo extensive background checks before being hired.

2. **Encryption**
    a. All data is strongly encrypted (minimum key length is 256 bits) in transit between:
        i. Customer and Apptoto (through website portal and API)
        ii. Apptoto and Subprocessors (through API)
        iii. All data is strongly encrypted at rest on disk.

3. **Security (System, Physical, Environmental)**
    a. All servers under control of Apptoto run virus detection software.
    b. All workstations under control of Apptoto run virus detection software.
    c. All personnel are required to leverage password managers and 2FA when available.
    d. All servers and databases are only accessible to operations personnel through VPN and Bastion gateways.

4. **Periodic Assessments**
    a. Periodic virus detection software assessment
    b. Periodic assessment of Acceptable Use Policy by personnel (see www.apptoto.com for Security Policy downloadable PDFs)
    c. Monthly web application security assessments through
        i. OWASP ZAP
        ii. Tinfoil Security Scanner

5. **Incident Response**
    a. (see www.apptoto.com for Security Policy downloadable PDFs)