DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is made between Cognito, LLC., a South Carolina corporation ("Cognito Forms") and {OrganizationLegalName} ("Customer" or "Controller" or "{Organization}") as an addendum to the Cognito Forms Terms of Service (the "Terms of Service"). This DPA is effective as of {AgreementDate} ("Effective Date"), which is the date {Organization} indicated its acceptance of this DPA electronically. This DPA was electronically signed by {RepresentativeName}, {RepresentativeTitle} on behalf of {Organization} on the Effective Date. Terms not otherwise defined below will have the meaning set forth in the Terms of Service.

{Organization} is a Controller of Personal Data collected via their forms and/or managed by their Account. Cognito Forms is the Processor of this data on behalf of {Organization}. {Organization} will be responsible for Controller obligations in this DPA and/or ensure that the Controller they work with fulfills these obligations. Specifically, {Organization} will ensure that:

- all applicable posted Privacy Policies permit use of Cognito Forms by {Organization},
- explicit authorization or consent has been obtained for use of Cognito Forms by {Organization} to process this Personal Data, and
- no additional agreements have been established that would prohibit use of Cognito Forms by {Organization}.

Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

1. Definitions

"Account" means the business arrangement between a Controller and Cognito Forms that authorizes the Controller to use Cognito Forms services in accordance with the Terms of Service. Each Account is represented as an "organization" in Cognito Forms, and this agreement applies to the organization {Organization}.

"Applicable Data Protection Laws" means all applicable laws and regulations relating to the processing of Personal Data and privacy that may exist in the relevant jurisdictions, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.

"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 Personal Data.

“Customer” means the Controller who has entered into the Terms of Service with Cognito Forms.

“Controller Personal Data” means Personal Data belonging to the Customer that is processed by Processor in the course of providing the Services under the Agreement.

“Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to Controller Personal Data.

“Data Subject” means the individual to whom Personal Data relates.

“EU Data Protection Law” means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the “GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom (the “UK”) any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union.

“Non-EU Data Protection Laws” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*., and its implementing regulations (“CCPA”) and Canada’s Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5 (“PIPEDA”) and any provincial legislation deemed substantially similar to PIPEDA pursuant to the procedures set forth therein, and all amendments to the CCPA, PIPEDA and similar legislation, as they may be enacted, from time to time.

“Personal Data” means any information relating to an identified or identifiable individual or as otherwise defined by Applicable Data Protection Law.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

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

"Services" means the services and other activities to be supplied to or carried out by or on behalf of Processor for the Controller pursuant to the Terms of Service.

“Standard Contractual Clauses” or “SCCs” means the clauses attached hereto as ANNEX pursuant to the European Commission’s decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Sub-processor" means any person appointed by or on behalf of Processor to Process Personal Data on behalf of the Controller in connection with the Terms of Service.

“Supervisory Authority” means any regulatory, supervisory, governmental or other competent authority with jurisdiction or oversight over compliance with the Applicable Data Protection Laws.

“Terms of Service” means the agreement between Cognito Forms and its Customer as set forth at https://www.cognitoforms.com/legal/terms.

2. Details of Data Processing

2.1 Subject Matter

The subject matter of the data processing under this DPA is the Controller Personal Data.

2.2 Duration

As between Cognito Forms and Customer, the duration of the data processing under this DPA is until the termination of this addendum in accordance with its terms.

2.3 Nature and Purpose

Controller Personal Data will be processed in accordance with our privacy policy (https://www.cognitoforms.com/legal/privacy) for the purpose of providing the services set out in the Terms of Service (including this DPA) or as otherwise agreed by the parties.

2.4 Types of Personal Data

Determined by Controllers to fulfill the purpose of their use of the Cognito Forms service.

2.5 Categories of Data Subjects

Any individual accessing and/or legally using the Services authorized through the Customer's Account. Any individual who uses the Services to submit personal data to the Controller.

3. Obligations and Rights of Controller

Within the scope of this DPA and the Terms of Service, {Organization} is the Controller of Personal Data, and Cognito Forms shall process Personal Data only as a data Processor acting on Controller’s behalf.

The Controller shall comply with its obligations as a Data Controller under Applicable Data Protection Laws in respect of its disclosure and transfer of Personal Data to the Processor, the processing of Controller Personal Data, and any processing instructions it issues. Controller shall process only data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective uses, including, but not limited to, providing notice and obtaining all consents and rights necessary under Applicable Data Protection Laws for Processor to process Controller Personal Data and provide the Services pursuant to the Terms of Service and this DPA.

Controller shall inform Processor comprehensively and without undue delay about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

4. Obligations and Rights of Processor

Processor shall process Personal Data only for the purposes described in this DPA and only in accordance with Controller's documented lawful instructions.

The parties agree that this DPA and the Terms of Service set out the Customer's complete and final instructions to Processor in relation to the processing of Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Controller and Processor.

If the Processor believes that an instruction of the Controller infringes Applicable Data Protection Law or requirements under this DPA, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the instructions due to a legal requirement under any Applicable Data Protection Law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by Applicable Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Controller Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Terms of Service for any failure to perform the applicable services until the Controller issues new instructions regarding the Processing.

5. Security

5.1 Security Measures

Processor shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from security incidents and to preserve the security and confidentiality of the Personal Data, in accordance with the security standards described in the Terms of Service and this DPA.

5.2 Updates to Security Measures

Controller is responsible for reviewing the information made available by Processor relating to data security and making an independent determination as to whether the Services meet Controller's requirements and legal obligations under Applicable Data Protection Laws. Controller acknowledges that the security measures are subject to technical progress and development and that Processor may update or modify the security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Controller.

5.3 Controller Responsibilities

Notwithstanding the above, Controller agrees that except as provided by this DPA, Controller is responsible for its secure use of the Services, including securing its Account authentication credentials, protecting the security of Personal Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Personal Data uploaded to the Services.

6. Confidentiality

Processor shall ensure that any personnel authorized to process Customer Data on its behalf, including employees, affiliates and sub-processors, is subject to confidentiality obligations, whether contractual or statutory, with respect to that Customer Data.

7. Personal Data Breach

In the event of a security breach which has resulted in (a) any unlawful access to any Controller Personal Data on the systems used to Process Controller Personal Data; or (b) any unauthorized access to Controller Personal Data, then Processor will notify Controller without undue delay and take reasonable steps to mitigate the effects and to minimize any damage resulting from the Data Breach.

In the event of a Data Breach, Processor shall provide the Controller with a description of the nature of the data breach and the affected Controller Personal Data and shall provide Controller with all reasonable assistance in relation to making a notification to a Supervisory Authority or any communication to Data Subject upon Customer's request as required under Applicable Data Protection Laws.

Processor's obligation to report or respond to a Data Breach under this Section is not and will not be construed as an acknowledgement by Processor of any fault or liability of Processor with respect to the Data Breach.

8. Data Subject Rights

Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under Applicable Data Protection Laws with respect to Controller Personal Data (including access, rectification, restriction, deletion or portability of Controller Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests. Controller shall reimburse Processor for the costs arising from this assistance.

9. Sub-processors

9.1 Authorized Sub-processors

Controller agrees that Processor may engage Sub-processors to process Personal Data on Controller's behalf. Sub-processors currently engaged by Cognito Forms and authorized by {Organization} are identified in the Cognito Forms Privacy Policy.

Processor shall enter into a written agreement with any Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standards required by Applicable Data Protection Laws and remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Processor to breach any of its obligations under this DPA.

9.2 Changes to Sub-processors

Processor shall maintain and make available in the Cognito Forms Privacy Policy an up-to-date list of the Sub-processors it has appointed, and will notify Controller (for which email shall suffice) if it adds or removes Sub-processors at least 10 days prior to any such changes. If the Controller objects to the changes in Sub-processors, the Controller' sole remedy will be to terminate their Account, thus terminating this DPA and the Terms of Service agreement and ending further Processing of Personal Data on their behalf.

10. Data Transfers

10.1 Transfer to United States

The Controller acknowledges that Processor may transfer and process Controller Personal Data to and in the United States and anywhere else in the world where Processor, Processor affiliates or its Sub-processors maintain data processing operations. Processor shall, at all times, ensure that such transfers are made in compliance with the requirements of all Applicable Data Protection Laws.

10.2 Standard Contractual Clauses

To the extent that Processor is a recipient of Controller Personal Data protected by EU Data Protection Laws ("EU Personal Data"), Processor agrees to abide by and Process EU Personal Data in compliance with the SCCs set forth in ANNEX to enable the lawful transfer of EU Personal Data. The parties further agree that the SCCs will apply to Controller Personal Data that is transferred via the Services from Europe to any location outside Europe, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Law). Where the parties have agreed to implement the SCCs, the Customer agrees that the SCCs, including any claims arising from them, are subject to the terms set out in the Agreement, including any exclusion and limitation of liability provisions. In any case of conflict between the Agreement and the SCCs, the latter shall prevail.

10.3 Data Processing Location

The Controller agrees that Processor and its Sub-processors may carry out data Processing operations in countries that are outside of the European Economic Area ("EEA") as necessary for the operation of the Services or to provide support-related services to, or other services requested by, the Customer. In the case of any non-EEA Processing, the transfer of Controller Personal Data will be subject to the transfer mechanisms set out in Section 10.2 above.

10.4 Alternative Mechanism

To the extent that Processor and the Controller are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently revoked, or held in a court of competent jurisdiction to be invalid, Processor will, in good faith, pursue a suitable alternate mechanism that can lawfully support the transfer.

11. Deletion or Retrieval of Controller Personal Data

Processor shall, at the choice of the Controller, delete or return all Controller Personal Data to the Controller after the end of the provision of services relating to processing. Controller must inform and instruct Processor on return of data in advance of terminating the agreement, as well a bear any additional cost arising with the return or deletion of Controller Personal Data.

If Controller terminates the Terms of Service, by deleting the organization {Organization}, without prior written notification to Processor, Processor will permanently delete all Controller Personal Data in its possession.

12. Audits

Controller may, upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor's business operations, conduct an on-site inspection of Processor's business operations to demonstrate Processor's compliance with this Addendum in relation to the Processing of the Company Personal Data, or have the same conducted by a qualified third party which shall not be a competitor of Processor.

Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party and provided that Controller not exercise this right more than once per year.

Controller may also review the SOC 2 Report or another audit of Provider's systems by an independent third party ("Third Party Audit"), if such a report is available.

Processor shall immediately inform Controller if, in its opinion, an instruction infringes upon Applicable Data Protection Laws.

13. Data Protection Impact Assessment

Upon Controller's request, Processor shall provide Controller with reasonable assistance needed to fulfill Controller's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment related to Controller's use of the Services, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Controller in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks to the extent required under the Applicable Data Protection Laws. Any reasonable costs arising from the provision of assistance by Processor under this Section 13 shall be borne by Controller. Processor shall provide an estimate of any such costs which shall be agreed in writing by the parties.

14. Order of Precedence

This DPA is incorporated into and forms part of the Terms of Service. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligations of the parties addressed under this DPA, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the SCCs, the SCCs will prevail.

15. CCPA

For purposes of the CCPA, the definitions of: "Controller" includes "Business"; "Processor" includes "Service Provider"; "Data Subject" includes "Consumer"; "Personal Data" includes "Personal Information"; in each case as defined under the CCPA. Cognito Forms is a Service Provider and

Customer is a Business (as the terms are respectively defined in the CCPA). Cognito Forms, as Service Provider, will not i) sell the Personal Data, or (ii) retain, use, or disclose the Personal Data for any purposes other than as described in the Agreement. Cognito Forms certifies that it understands these restrictions and shall comply with them.

16. Limit of Liability

Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Terms of Service. For the avoidance of doubt, Processor's and its affiliates' total liability for all claims from the Customer arising out of the Terms of Service and each DPA shall apply in the aggregate for all claims under both the Terms of Service and all DPAs established under the Terms of Service.

Agreement Date: {AgreementDate}

{OrganizationLegalName}

By:

{Signature}

{RepresentativeName}

{RepresentativeTitle}

Cognito, LLC

By:

Jamie Thomas

Co-founder

ANNEX

STANDARD CONTRACTUAL CLAUSES

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) 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;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(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 the 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 Union4 (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.

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 noncompliance. 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 ten (10) 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. 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.

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

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.

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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:

1. 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;
2. 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;
3. 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.

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.

SECTION IV – FINAL PROVISIONS

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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Czech Republic.

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 the Member State in which the data exporter is established.

(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

A. LIST OF PARTIES

Data exporter(s):

Name: {User.Organization}

Address: {OrganizationAddress}

Contact person's name, position and contact details: {RepresentativeName}, {RepresentativeTitle}, {User.Email}

Activities relevant to the data transferred under these Clauses: Data exporter uses Cognito Forms to collect and process information to support the needs of their organization. Cognito Forms transfers this information solely to fulfill these needs.

Signature and date: {Signature} {AgreementDate}

Role (controller/processor): Controller

Data importer(s):

Name: Cognito Forms

Address: 929 Gervais Street Suite D, Columbia, SC 29201.

Contact person's name, position and contact details: Jamie Thomas, Privacy Officer, privacy@cognitoforms.com

Activities relevant to the data transferred under these Clauses: The processing activities set out under Section 2 of the Data Processing Agreement to which the Clauses are attached.

Signature and date: Jamie Thomas {AgreementDate}

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Any individual accessing and/or legally using the Services authorized through the Customer's Account. Any individual who uses the Services to submit personal data to the Controller.

Categories of personal data transferred

Those categories as determined by Controllers to fulfill the purpose of their use of the Cognito Forms service.

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.

The parties do not anticipate the transfer of sensitive data.

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

Continuous basis as determined by Data Exporter.

Nature of the processing

Controller Personal Data will be processed in accordance with Processor's privacy policy (https://www.cognitoforms.com/legal/privacy) for the purpose of providing the services set out in the Terms of Service or as otherwise agreed by the parties.

Purpose(s) of the data transfer and further processing

Controller Personal Data will be processed for the purpose of providing the services set out in the Terms of Service or as otherwise agreed by the parties.

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

Data will be retained until a request for deletion is initiated by the Data Exporter plus thirty (30) days. At the time of deletion, data will no longer be accessible or recoverable and will be purged from all systems within 30 days.

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

Sub-processors (Third Parties) data transfer are described here: https://www.cognitoforms.com/legal/privacy#authorized-third-parties

C. COMPETENT SUPERVISORY AUTHORITY

The Local Supervisory Authority for the Member State in which the data exporter is established.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The Security Measures applicable to the Services are described here:

1. Cognito Forms uses TLS 1.2/SSL encryption and is always accessed over HTTPS 100% of the time for all users.
2. Cognito Forms is hosted securely on the Microsoft Azure cloud platform, which is PCI (DSS) Level 1 and HIPAA compliant.
3. Access to our production environment is limited to select operations security staff, requiring two-factor authentication to deploy updates or access a secure system for limited troubleshooting.
4. We do not look at entry data for our customers unless requested to through an official support request. The details of our concern over data privacy are detailed in our Privacy Policy.
5. Customer data is carefully segregated at the lowest architectural level in Cognito Forms to ensure that data for one organization cannot be accessed by another.
6. We partner with PayPal, Stripe, and Square for credit card processing so that secure payment information is never transmitted or stored by Cognito Forms. We also take measures to prevent malicious scripts on sites we are embedded in from stealing this information.
7. The Cognito Forms architecture is unique and highly specialized for massive scale while maintaining data isolation. It does not use transactional databases and is not vulnerable to SQL injection attacks.

8. Production access credentials for storage and encryption tokens used to encrypt sensitive organization data are stored in an Azure credential store and are not stored within our own development environments.
9. All text data stored by Cognito Forms is sanitized to prevent JavaScript injection attacks, which someone might attempt to leverage by submitting JavaScript as entry data to maliciously access other entry data by compromising our customers browsers when managing entries.
10. Sensitive data, such as Social Security numbers and other personally identifiable information, is required to be encrypted at rest using 256-bit AES encryption. It must also be protected so that it is never emailed or otherwise transmitted in an insecure way. Any field type can be encrypted and/or protected, including uploaded files and sections.
11. Cognito Forms uses opportunistic TLS encryption when sending email to always encrypt messages when supported by downstream servers.
12. Cognito Forms customers can enable two-factor authentication (2FA) to add a second login step to their account. Additionally, organizations on the Enterprise plan level can require two-factor authentication for all users.
13. Cognito Forms has an internal Security Policy which is reviewed annually, all employees are required to agree, and represents safeguards for onboarding and offboarding of employees, risk management, access levels, password requirements, workstations/devices, anti-virus protection, two-factor authentication, software development lifecycle, and disaster recovery.