



## 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 {AgreementDateFormatted} (“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 Privacy Framework” (DPF)** means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, as administered by the U.S. Department of Commerce, which provide a valid legal mechanism for the transfer of Personal Data from the European Union, United Kingdom, and Switzerland to the United States in compliance with applicable data protection laws and regulations.

**“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.

**“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 Reliance on the Data Privacy Framework (DPF)**

The Processor is certified under the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF (UK DPF), and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). These frameworks enable the lawful transfer of Personal Data to the United States from the European Union, United Kingdom, and Switzerland, respectively. The Processor shall process such Personal Data in accordance with the principles of the DPF as applicable to each jurisdiction. In the event of any conflict between this DPA and the DPF principles, the DPF principles shall govern with respect to such data transfers.

## **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"), the United Kingdom, and Switzerland as necessary for the operation of the Services or to provide support-related services to, or other services requested by, the Customer. In such cases, the Processor shall rely on the DPF or other appropriate transfer mechanisms under Applicable Data Protection Laws to ensure lawful data transfers.

## **10.4 Alternative Mechanism**

To the extent that Processor and the Controller are relying on the DPF or any other 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 as 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 any conflict between this DPA and the DPF Principles, the DPF Principles shall take precedence for data transfers

covered by the scope of the frameworks. If the DPF is revoked or invalidated, the Processor will comply with Section 10.4 regarding the implementation of alternative transfer mechanisms.

## 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:** {AgreementDateFormatted}

**{OrganizationLegalName}**

**By:**

{Signature}

{RepresentativeName}

{RepresentativeTitle}

**Cognito, LLC**

**By:**

Jamie Thomas

Co-founder