# SnapApp Data Processing Agreement

This Data Processing Addendum ("**DPA**") is entered into by and between SnapApp, Inc. ("**SnapApp**") and _____ (Customer) and forms part of the services agreement(s) previously entered into by and between SnapApp and Customer (the "**Agreement**").

SnapApp agrees that it shall comply with the following provisions with respect to all "**Personal Information**" collected, used, transmitted or maintained for Customer. This Addendum stipulates privacy, confidentiality, and security requirements and demonstrates compliance with applicable privacy, security and data protection laws. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the event of a conflict between this DPA and the Agreement, this DPA will control, but only to the extent of the conflict. This DPA shall only become legally binding between SnapApp and Customer upon Customer's execution of this DPA. This DPA *may be executed* in two or more *counterparts*, including facsimile or e-mail counterparts, which together shall constitute a single agreement.

**1. Definitions.**

(a) "**EEA Personal Data**" means personal data (as defined in GDPR) pertaining to residents of the European Economic Area (EEA) and Switzerland.

(b) "**GDPR**" means Regulation (EU) 2016/679, the General Data Protection Regulation.

(c) "**Personal Information**" means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, "personal data" (as defined in the GDPR) and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location.

(d) "**Privacy Laws**" means all applicable U.S. and international laws that regulate the Processing of Personal Information. In particular, "Privacy Laws" includes the GDPR and other applicable laws that specify privacy, security or security breach notification obligations that affect the Personal Information or the provision of the Services by SnapApp.

(e) "**Processing**" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.

(f) "**Security Breach**" means a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law or any other event that compromises the security, confidentiality or integrity of Personal Information.

(g) "**Services**" means any and all services that Customer requests SnapApp to perform under the Agreement or any other contract or agreement that involves Processing of Personal Information.

(h) "**Subprocessor**" means any third party (including an affiliate of SnapApp) that provides any services to SnapApp and that may have access (including inadvertent access) to any Customer Personal Information.

(i) "**Transfer**" means to disclose or otherwise make the Personal Information available to a third party (including to any affiliate or Subprocessor of SnapApp), either by physical movement of the Personal Information to such third party or by enabling access to the Personal Data by other means.

(j) "**Customer Personal Information**" means any Personal Information Processed by a SnapApp on behalf of a Customer pursuant to or in connection with the Agreement;

**2. General Obligations.**

(a) SnapApp shall only Process or Transfer Personal Information as authorized by Customer and as necessary to perform the Services.

(b) SnapApp shall promptly inform Customer in writing: (i) if it cannot comply with any material term of its Agreement with Customer regarding the Services (if this occurs, SnapApp shall use reasonable efforts to remedy the non-compliance, and Customer shall be entitled to terminate SnapApp's further Processing of Personal Information); (ii) of any request for access to any Customer Personal Information received from an individual who is (or claims to be) the subject of the data; (iii) of any request for access to any Customer Personal Information received by SnapApp from any government official (including any data protection agency or law enforcement agency) unless it is explicitly prohibited by law from notifying Customer of the request; (iv) of any other requests with respect to Customer Personal Information received from Customer's employees or other third parties, other than those set forth in the agreement.

(c) Each party must use reasonable efforts to stay informed of the legal and regulatory requirements for its Processing of Personal Information. SnapApp's Processing shall comply with all Privacy Laws that are applicable to the Processing, as well as SnapApp's own privacy notices. SnapApp certifies that it is now and shall remain in compliance with all applicable Privacy Laws.

(d) SnapApp will provide Customer with responses to Customer's Vendor Due Diligence Questionnaire, as requested, along other information as needed to support those responses. SnapApp represents and warrants that all such responses and information were accurate, current and complete, in all material respects.

(e) Once annually upon Customer's written request, SnapApp shall provide Customer with copies of applicable internal reports regarding its security policies and procedures. Customer understands that the responses and internal reports contain Confidential Information of the SnapApp, and it shall not disclose such information other than to its auditors and advisors in connection with verifying SnapApp's compliance with Customer's security and privacy program requirements.

(f) If the Customer Personal Information will include EEA Personal Data, SnapApp and Customer shall ensure adequate protection for the EEA Personal Data. Each party shall comply with the provisions of GDPR and other Privacy Laws applicable to it, as a "controller" or a "processor" (as defined in GDPR. In the event of any Transfers of EEA Personal Data, the parties shall document adequate protection for the EEA Personal Data using another approved means in accordance with section 4(c) below.

(g) SnapApp shall reasonably cooperate with Customer and with its affiliates and representatives in responding to inquiries, incidents, claims and complaints regarding the Processing of the Customer Personal Information or as otherwise needed for Customer to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws.

**3. Confidentiality and Data Access.**

(a) SnapApp may disclose Personal Information to its employees and contingent workers, but only to the extent such individuals require access to the Customer Personal Information to perform the Services.

(b) Prior to allowing any employee or contingent worker to Process any Personal Information, SnapApp shall require the individual to execute an enforceable confidentiality agreement and provide the individual with appropriate privacy and security training. SnapApp will also monitor its employees for compliance with the privacy and security program requirements.

**4. Approvals for Transfers and Subprocessors.**

(a) SnapApp shall not Transfer the Customer Personal Information to any Subprocessors or other third parties unless such Processing is required to perform the Services

(b) Notwithstanding the preceding paragraph, Customer understand that SnapApp has a contractual relationship with the following Subprocessor(s):

| **Subprocessor:** | **Services Provided:** | **Location:** |
|---|---|---|
| Amazon Web Services | IAAS | USA - various |

Customer further understands that such Subprocessor(s) is/are bound by contract containing terms materially the same as those contained herein that requires it to protect all SnapApp information to which it may be exposed. Customer authorizes SnapApp to make routine transfers of Personal Information in the normal course of business on its corporate systems to Subprocessor(s).

(c) SnapApp shall not Transfer the Personal Information across any national borders or permit remote access to the Personal Information from any employee, contingent worker, affiliate, Subprocessor(s) or other third party outside of the country unless SnapApp has the prior written consent of Customer for such Transfer.

(d) Notwithstanding the preceding paragraph, Customer authorizes SnapApp to make routine Transfers of Personal Information in the normal course of business on its corporate systems to itself in the USA. To the extent that these Transfers include any EEA Personal Data, SnapApp agrees to comply with the provisions paragraph (e) below regarding the Transfers of EEA Personal Data.

(e) SnapApp has certified its compliance to the EU-US Privacy Shield Program. SnapApp shall maintain its certification to the Privacy Shield for so long as it maintains any EEA Personal Data. In the event that EU authorities or courts determine that the Privacy Shield is not an appropriate basis for transfers, SnapApp and Customer shall promptly take all steps reasonably necessary to demonstrate adequate protection for the EEA Personal Data, using another approved mechanism. SnapApp understands and agrees that Customer may terminate the Transfers as needed to comply with the EEA Privacy Laws.

**5. <u>Information Security Requirements</u>.**

(a) SnapApp shall have implemented and documented appropriate administrative, technical and physical measures set forth in the Agreement, as applicable, to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. SnapApp will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. SnapApp will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that these risks are addressed.

(b) SnapApp shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it continue or resume providing Services (including restoring access to the Personal Information) in a timely manner after a disruptive event. SnapApp will regularly test and monitor the effectiveness of its business continuity and disaster recovered plans. At appropriate intervals or as otherwise requested by Customer, SnapApp will provide a copy of its written business continuity and disaster recovery plans to Customer.

(c) If the Processing involves the transmission of Personal Information over a network, SnapApp shall have implemented appropriate supplementary measures to protect the Personal Information against the specific risks presented by the Processing. Personal Information may not be transmitted over any insecure network unless it has been appropriately encrypted.

(d) Personal Information may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks, USB or flash drives, personal digital assistants (PDAs) or mobile phones, DVDs, CDs or computer tapes) unless it is encrypted.

(e) Upon request, SnapApp shall provide Customer with information about SnapApp's information security program. SnapApp shall also submit its owned data processing facilities for annual audit during SnapApp's reasonable business hours, which shall be carried out by Customer (or by an independent auditor designated by Customer) in a mutually-agreeable manner no more than ten (10) day after any such request. SnapApp shall fully cooperate with any such audit. In the event that any such audit reveals material gaps or weaknesses in SnapApp's security program, Customer shall be entitled to terminate SnapApp's Processing of Customer Personal Information until such issues are resolved. Such audits will be limited to once per year; provided however, that Customer may audit at any time in the event of a security breach or suspected material violation by SnapApp of its obligations under the Agreement or this DPA. SnapApp shall also cooperate with any audits conducted by any regulatory agency that has authority over Customer as needed to comply with applicable law.

(f) SnapApp will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of Customer Personal Information. SnapApp will notify Customer within twenty-four (24) hours upon discovery of any Security Breach. Notifications should be sent via e-mail to _____. SnapApp shall provide Customer with all information about the Security Breach reasonably needed by Customer to assess its incident response obligations. Such notification shall as a minimum (i) describe the nature of the Security Breach, the categories and numbers of data subjects concerned, and the categories and numbers of personal data records concerned; (ii) communicate the name and contact details of SnapApp's data protection officer or other relevant contact from whom more information may be obtained; (iii) describe the likely consequences of the Security Breach; and (iv) describe the measures taken or proposed to be taken to address the Security Breach.

(g) SnapApp shall bear all costs associated with resolving a Security Breach, including (without limitation), conducting an investigation, engaging appropriate forensic analysis, notifying individuals, regulators and others as required to by law.

(h) When SnapApp ceases to perform Services for Customer (and at any other time, upon request), SnapApp will either, at Customer's option (i) return the Personal Information (and all media containing copies of the Personal Information) to Customer, or (ii) with Customer's prior written consent, purge, delete and destroy the Personal Information. Electronic media containing Personal Information will be disposed of in a manner that renders the Personal Information unrecoverable. SnapApp will provide Customer with an Officer's Certificate to certify its compliance with this provision. If SnapApp is required by applicable law to retain any Personal Information, SnapApp warrants that it shall (i) ensure the continued confidentiality and security of the Personal Information, (ii) securely delete or destroy the Personal Information when the legal retention period has expired, and (iii) not actively Process the Personal Information other than as needed for to comply with law.

(i) SnapApp shall carry appropriate insurance to address the risks from its Processing of the Personal Information, including risks of cyber-attacks and security breaches.

**IN WITNESS WHEREOF,** the parties have executed this DPA by their respective, duly authorized officers.

| **SNAPAPP, INC.** | **CUSTOMER** |
|---|---|
| By: _____ | By: _____ |
| Name: Russell Franks | Name: _____ |
| Title: President & COO | Title: _____ |
| Date: | Date: _____ |