

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is incorporated by reference into the Client Agreement ("Agreement") between Customer (as identified in the Agreement) and Paminga, Inc. ("Paminga"). This DPA is effective as of the effective date of the Agreement.

Under the Agreement, Paminga may process Personal Data (defined herein) on behalf of Customer. This DPA serves to define the terms under which Paminga will process Personal Data, and to ensure that such processing is conducted in adherence with applicable laws including the European Union's General Data Protection Regulation ("GDPR", defined herein).

DATA PROCESSING TERMS

In providing the Subscription Services to Customer pursuant to the Agreement, Paminga may Process Personal Data on behalf of Customer. Paminga will comply with the provisions in this DPA with respect to its Processing of any Personal Data. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1. Definitions

- a. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.



- b. "Controller" means the entity that determines the purposes and means of the Processing of Personal Data.
- c. "Customer" means the party identified as the Customer in the Agreement.
- d. "Customer Data" means any data, information or material originated by Customer that Customer submits to Paminga, collects through its use of the Subscription Services or provides to Paminga in the course of using the Subscription Services.
- e. "Data Protection Laws and Regulations" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including the GDPR, the UK GDPR, the Swiss FADP, and any implementing or successor legislation.
- f. "Data Subject" means the identified or identifiable person to whom Personal Data relates.
- g. "EEA" means the European Economic Area (the member states of the European Union plus Norway, Iceland and Liechtenstein).
- h. "GDPR" means Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as amended, replaced or superseded.
- i. "UK GDPR" means the GDPR as incorporated into the law of the United Kingdom by the Data Protection Act 2018 and the European Union (Withdrawal) Act 2018, as amended.
- j. "Swiss FADP" means the Swiss Federal Act on Data Protection, as revised, and its implementing ordinances.



- k. "Personal Data" means any Customer Data relating to an identified or identifiable natural person.
- l. "Data Privacy Framework" or "DPF" means the EU–US Data Privacy Framework (and, as applicable, the UK Extension and the Swiss–US DPF) administered by the U.S. Department of Commerce, together with the DPF Principles, in each case only where and while Paminga maintains an active self-certification.
- m. "Restricted Transfer" means a transfer of Personal Data to, or access to Personal Data from, a country outside the EEA, the United Kingdom or Switzerland that is not the subject of an adequacy decision or determination.
- n. "Processor" means an entity which processes Personal Data on behalf of the Controller.
- o. "Processing" means any operation performed on Personal Data, whether or not by automated means, such as collection, recording, storage, use, disclosure, erasure or destruction.
- p. "Subscription Services" means the marketing automation services provided to Customer by Paminga per the Agreement.
- q. "Sub-processor" means any Processor engaged by Paminga.
- r. "Supervisory Authority" means an independent public authority established under Data Protection Laws and Regulations.
- s. "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (Controller to Processor), as completed in Exhibit 1.



- t. "UK Addendum" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under s.119A of the Data Protection Act 2018, as completed in Exhibit 1.
- u. "Technical and Organizational Measures" or "TOMs" means the measures described in Annex II to Exhibit 1.

2. Roles and Responsibilities

- a. The parties agree that Customer is the Controller and Paminga is the Processor with regard to the Processing of Personal Data. Where Customer is itself a processor acting on behalf of a third-party controller, Paminga acts as sub-processor and this DPA applies accordingly.
- b. Customer shall, in its use of the Services, Process Personal Data in accordance with Data Protection Laws and Regulations, and is solely responsible for the accuracy, quality, and legality of Personal Data and the means by which it was acquired, and for the lawfulness of its processing instructions.
- c. Paminga shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions, including as set out in the Agreement, in Customer's use of the Subscription Services, and via other reasonable documented instructions, unless required to process by applicable law (in which case Paminga shall, where legally permitted, inform Customer).
- d. Training. Paminga shall ensure that its relevant employees, agents and contractors receive appropriate training regarding the Processing, protection and confidentiality of Personal Data.



3. Data Subject Requests

Paminga shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise rights of access, rectification, restriction, erasure, data portability, objection, or the right not to be subject to automated decision-making (a “Data Subject Request”). Taking into account the nature of the Processing, Paminga shall assist Customer by appropriate technical and organizational measures, insofar as possible, to fulfil Customer’s obligation to respond. Where Customer cannot address a Data Subject Request through its use of the Services, Paminga shall provide commercially reasonable assistance on written request, to the extent legally permitted. Customer is responsible for responding to Data Subject Requests and, to the extent legally permitted, for the costs of Paminga’s assistance.

4. Security

- a. Paminga shall implement and maintain the Technical and Organizational Measures set out in Annex II to Exhibit I, designed to ensure a level of security appropriate to the risk, taking into account the state of the art, costs of implementation, and the nature, scope, context and purposes of Processing. Paminga will not materially decrease the overall security of the Services during a subscription term.
- b. Confidentiality. Paminga shall ensure that personnel authorized to Process Personal Data are subject to a duty of confidentiality that survives termination of their engagement.
- c. Security Incidents. Upon becoming aware of a Security Incident, Paminga shall notify Customer without undue delay, and shall provide information reasonably available to Paminga to enable Customer to meet its own breach-notification obligations.



Paminga shall take reasonable steps to identify the cause and remediate it to the extent within Paminga's reasonable control. This obligation does not apply to incidents caused by Customer or its Users.

5. Sub-processing

- a. Customer authorizes Paminga to engage Sub-processors to Process Personal Data. Current Sub-processors are listed in Annex III to Exhibit 1 and at Paminga's Sub-processor page: <https://www.paminga.com/legal/sub-processor-list/>.
- b. Notice of new Sub-processors. Paminga shall provide notice of any intended addition or replacement of a Sub-processor at least ten (10) business days before that Sub-processor begins Processing Personal Data, by updating the Sub-processor page and (where Customer has provided an email/subscription contact) by email. Paminga shall make a subscription mechanism available; the absence of a subscription does not relieve Paminga of its obligation to post notice.
- c. Objection. Customer may object on reasonable data-protection grounds within ten (10) business days of notice by emailing legal@paminga.com. The parties will work in good faith to resolve the objection; if Paminga cannot reasonably avoid the objected-to Sub-processor within thirty (30) days, Customer may terminate the affected Subscription Services and receive a pro-rata refund of prepaid fees for the terminated portion, without penalty.
- d. Emergency replacement. Paminga may replace a Sub-processor where urgent and necessary and beyond its reasonable control,



notifying Customer as soon as practicable; Customer retains the objection right above.

- e. Flow-down and liability. Paminga shall impose data-protection obligations on each Sub-processor that are no less protective than those in this DPA and shall remain liable for the acts and omissions of its Sub-processors.

6. Audits

Paminga shall make available information necessary to demonstrate compliance with this DPA and Article 28 GDPR, including its then-current SOC 2 and/or ISO 27001 reports. On reasonable prior written notice, no more than once per twelve (12) months (unless required by a Supervisory Authority or following a Security Incident), Customer may audit the architecture, systems and procedures relevant to the protection of Personal Data, subject to confidentiality and to mutually agreed scope, timing and duration. Customer shall reimburse Paminga's reasonable costs for on-site audits at its then-current professional services rates. This section satisfies Clause 8.9 of the SCCs.

7. Cooperation

- a. Supervisory Authorities. Paminga shall notify Customer without undue delay if a Supervisory Authority or law enforcement authority makes an inquiry or request for disclosure regarding Personal Data, unless legally prohibited.
- b. DPIAs. Paminga shall provide reasonable assistance with data protection impact assessments and prior consultations required of Customer under Data Protection Laws and Regulations, to the extent the relevant information is available to Paminga and not otherwise available to Customer.



8. Deletion or Return of Customer Data

Upon termination or expiration of the Agreement, Paminga shall, at Customer's choice, delete or make available for retrieval all Personal Data (including copies) in its possession, and delete existing copies within a reasonable period (not to exceed ninety (90) days) unless retention is required by applicable law, in which case Paminga shall protect the Personal Data and limit further Processing to the purpose(s) requiring retention.

9. International Data Transfers

- a. Application. This section applies whenever Processing under the Agreement involves a Restricted Transfer of Personal Data protected by the GDPR, UK GDPR or Swiss FADP.
- b. EU SCCs (primary mechanism). The parties agree that the Standard Contractual Clauses (Module Two, Controller to Processor) apply to Restricted Transfers from the EEA and are incorporated by reference and completed as follows:
 - i. Clause 7 (docking clause) applies;
 - ii. Clause 9 – Option 2 (general written authorization) applies, with the notice period in Section 5 of this DPA;
 - iii. Clause 11 optional independent-redress language does not apply;
 - iv. Clause 17 (governing law): the law of Ireland;
 - v. Clause 18 (forum): the courts of Ireland;



- vi. Annex I, II and III are set out in Exhibit 1. In case of conflict, the SCCs prevail over the rest of this DPA for the Restricted Transfer they govern.
- c. UK transfers. For Restricted Transfers subject to the UK GDPR, the UK Addendum is incorporated by reference and completed in Exhibit 1, appending to and amending the EU SCCs.
- d. Swiss transfers. For Restricted Transfers subject to the Swiss FADP, the EU SCCs apply with the following amendments: references to the GDPR are to the FADP; the competent authority is the Swiss FDPIC; and 'member state' references do not prevent data subjects in Switzerland from bringing claims in their place of habitual residence.
- e. Data Privacy Framework
Paminga shall become and remain self-certified under, and shall comply with, the EU-US Data Privacy Framework, the UK Extension to the EU-US DPF, and the Swiss-US DPF (collectively, the "DPF") as administered by the U.S. Department of Commerce, with respect to Personal Data transferred from the EEA, the United Kingdom and Switzerland. Paminga shall:
 - i. maintain an active DPF self-certification for as long as it relies on the DPF to receive such Personal Data;
 - ii. Process such Personal Data in accordance with the DPF Principles, including the Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability Principles;



- iii. provide at least the same level of protection as the DPF Principles require where it engages a Sub-processor as an agent to Process such Personal Data, and remain liable under the Accountability for Onward Transfer Principle;
 - iv. promptly notify Customer if it can no longer meet this obligation or if its certification lapses or is withdrawn, and in that event either cease Processing or take reasonable and appropriate steps to remediate; and
 - v. acknowledge that it remains subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission. For any period during which Paminga's DPF certification is not active, the Standard Contractual Clauses above (and the UK and Swiss mechanisms above) apply automatically as the transfer mechanism without further action by either party.
- f. Transfer impact and government access. Each party warrants it has no reason to believe the laws applicable to Paminga prevent it from meeting its obligations under the SCCs. Paminga shall, to the extent legally permitted, notify Customer of any legally binding request by a public authority for Personal Data, challenge requests it considers unlawful, and provide the information required by Clauses 14 and 15 of the SCCs. The parties will document a transfer impact assessment on request.

10. US State Privacy Terms

Where Customer is subject to the California Consumer Privacy Act, as amended by the CPRA, or comparable US state privacy laws, Paminga acts as a “service provider”/“processor” and shall: (a) Process personal information only to provide the Services and for the business purposes



in the Agreement; (b) not “sell” or “share” personal information and not retain, use or disclose it outside the direct business relationship or for any purpose other than those specified; and (c) notify Customer if it determines it can no longer meet these obligations. Customer may take reasonable steps to remediate unauthorized use.

11. Limitation of Liability

Each party’s liability arising out of or related to this DPA, whether in contract, tort or otherwise, is subject to the “Limitation of Liability” section of the Agreement. Nothing in this DPA limits either party’s liability to Data Subjects under the third-party beneficiary rights of the SCCs.

12. Miscellaneous

- a. By entering into the Agreement, each party is deemed to have executed and agreed to be bound by this DPA, the Standard Contractual Clauses, and the UK Addendum if applicable, including their Annexes and Tables, as of the effective date of the Agreement.
- b. Except as amended by this DPA, the Agreement remains in full force and effect.
- c. If there is a conflict between the Agreement and this DPA, this DPA controls; for Restricted Transfers governed by the SCCs, the SCCs control.
- d. Claims under this DPA are subject to the exclusions and limitations in the Agreement.
- e. Customer may terminate this DPA and the SCCs on written notice where required to comply with Data Protection Laws and Regulations.





EXHIBIT 1 — STANDARD CONTRACTUAL CLAUSES (2021/914) — COMPLETED ANNEXES

The EU SCCs (Implementing Decision (EU) 2021/914), Module Two, are incorporated by reference. The parties complete their Annexes as follows.

Annex I — Parties and Description of Processing

A. Parties.

a. **Data exporter:**

The Customer as identified in the Agreement, acting as controller.

b. **Data importer:**

Paminga, Inc.

6698 South Iris Street #621149

Littleton, CO 80162, USA

contact legal@paminga.com, acting as processor

B. Description. Categories of data subjects: Customer's customers, contacts and prospects; employees/contractors of those parties; and Customer's own employees and contractors. Categories of Personal Data: name, employer, business role/title, contact information (email, phone, address), business network/experience/interests, localization data, and device identifiers. Special categories: none intended; determined solely by Customer's configuration. Frequency: continuous, for the term of the Agreement. Nature/purpose: provision of the marketing automation Subscription Services (collection, recording, organization, storage, use, disclosure, transmission, retrieval, and deletion). Retention: for the term plus deletion per Section 8.



C. Competent supervisory authority: the authority of the EU member state selected under Clause 17 (the Irish Data Protection Commission).



Annex II — Technical and Organizational Measures

Paminga maintains the following measures (as evidenced in its SOC 2 Type II and ISO 27001 program):

- Encryption: TLS/HTTPS for data in transit; AES-256 encryption for customer data at rest; endpoint (disk) encryption on devices accessing in-scope data.
- Access control: role-based access on a least-privilege, need-to-know basis; multi-factor authentication on critical systems; privileged accounts via password vault; quarterly access reviews; timely deprovisioning on termination; auto screen-lock.
- Network security: AWS Virtual Private Cloud with deny-by-default security groups/firewalls; network segmentation; IDS/IPS and capacity/DDoS monitoring; only validated ports/protocols permitted; admin access via SSH/VPN only.
- Hosting & physical security: production hosted on AWS (US regions); physical and environmental controls inherited from AWS and reviewed annually.
- Vulnerability & patch management: at least monthly vulnerability scanning; automated patching; risk-ranked remediation; secure-coding review and mandatory peer code review via version control.
- Logging & monitoring: audit logging for critical systems; anomaly/threat detection; continuous compliance monitoring (Sprinto).
- Resilience: at least daily backups; backup restoration tested at least annually; documented Business Continuity/Disaster Recovery plan with RTO/RPO testing.



- Endpoint protection: managed endpoints with anti-malware and email-attachment scanning; enforced OS updates and encryption.
- Personnel: background checks; confidentiality agreements; security and privacy awareness training on hire and at least annually.
- Incident management: documented incident-response framework with severity ratings, post-mortems for critical incidents, and a data-breach notification policy.
- Data governance: data classification (customer data classified confidential); Records of Processing Activities; data retention and secure media-disposal policies.



Annex III — List of Sub-processors

- Amazon Web Services, Inc. (AWS) — cloud hosting/infrastructure — USA
- Twilio SendGrid — transactional/marketing email delivery — USA
- Paubox, Inc. — encrypted email delivery when required — USA

Current list maintained at

<https://www.paminga.com/legal/sub-processor-list/>



UK Addendum

Field	Exporter	Importer
Role	Controller	Processor
Party	Customer	Paminga, Inc.
Full legal name	Customer as identified in the Agreement	Paminga, Inc.
Address	Customer as identified in the Agreement	6698 South Iris Street #621149 Littleton, CO 80162 USA
Contact	Customer as identified in the Agreement	Paminga Legal Team legal@paminga.com
Key contact	Customer as identified in the Agreement	Paminga Legal Team legal@paminga.com



Table 2: Selected SCCs, Modules and Selected Clauses

The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: the standard contractual clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

Approved EU SCCs version	Commission Implementing Decision (EU) 2021/914 of 4 June 2021
Date	as of the effective date of the DPA
Reference	Paminga Data Processing Addendum, Section 9 and Exhibit 1
Other identifier	None
Modules in operation	Module Two (Controller to Processor)
Clause 7 (Docking Clause)	Used
Clause 9a (authorisation)	General Authorisation (Option 2)
Clause 9a (time period)	As set out in Section 5 of the DPA
Clause 11 (independent dispute resolution)	Not used
Data received from Importer combined with data collected by Exporter	No
Clause 17 (Governing law)	Ireland
Clause 18 (Forum and jurisdiction)	Ireland

Reference: Paminga Data Processing Addendum, Section 9 and Exhibit 1.



Table 3: Appendix Information

Appendix	Value
Annex 1A (List of Parties)	As set out in Annex I of Exhibit 1 to the DPA
Annex 1B (Description of Transfer)	As set out in Annex I of Exhibit 1 to the DPA
Annex II (Technical and organisational measures)	As set out in Annex II of Exhibit 1 to the DPA
Annex III (List of Sub-processors)	As set out in Annex III of Exhibit 1 to the DPA

Table 4: Ending this Addendum when the Approved Addendum changes

Which Parties may end this Addendum as set out in Section 19	Selection
Importer	Neither
Exporter	Neither