ArcPrime Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms a part of the ArcPrime Terms of Service at https://www.arcprime.com/terms (the "**Agreement**"). This DPA is effective as of the date last signed below ("**Effective Date**") and is by and between the company identified in the signature block below ("**Customer"**) and ArcIP, Inc. ("**ArcPrime**"). Customer is the Controller of certain personal data, and wishes to appoint ArcPrime as a Processor to process personal data on its behalf in connection with ArcPrime's performance of the services ("**Services**") described in the Agreement.

1. Definitions.

"**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.

"**EU Data Protection Law**" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Data Protection Laws"** means any and all privacy, security and data protection laws and regulations that apply to Personal Data Processed by ArcPrime under the Master Agreement, including, as applicable, the EU Data Protection Law, the UK GDPR and the CCPA.

"**Personal Data**" means any information relating to an identified or identifiable natural person as defined under Data Protection Laws that Customer provides or makes available to ArcPrime as part of the Services.

"**Process**", "**Processing**", "**Processor**", "**Controller**", and "**Data Subject**" have the meanings set forth in the EU Data Protection Law.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Services**" means the services provided by ArcPrime as specified in the ordering document and Agreement executed by the parties.

"**Standard Contractual Clauses**" means, as applicable, (i) the Standard Contractual Clauses adopted by the European Commission pursuant to its Implementing Decision (EU) 2021/914 of 4 June 2021, including all modules governing controller to processor transfers of personal data, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in Section 3 (International Transfers of Personal Data) and as set forth in the Annexes to this DPA (the "**EU SCCs**"); and (ii) the International Data Transfer Addendum to the EU Standard Contractual Clauses adopted by the UK Information Commissioner's Office effective March 21, 2022 and completed as described in Section 3 (International Transfers of Personal Data) (the "**UK SCCs**").

"**UK GDPR**" means EU Data Protection Law as implemented by the United Kingdom pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

2. Processing of Personal Data.

2.1. This Agreement applies when Personal Data is Processed by ArcPrime on behalf of Customer. As between Customer and ArcPrime, at all times Customer will act as the "Controller" and ArcPrime will act as the "Processor" with respect to the Personal Data.

2.2. The subject matter of the Processing under this DPA is Personal Data provided to ArcPrime by Customer. The duration of the Processing under this DPA is for the term of this DPA and the Agreement. The purpose of the Processing of Personal Data under this DPA is for ArcPrime to provide the Services to Customer. The nature of the Processing is the provision of the Services by ArcPrime and as more specifically described in the ordering document and the Agreement. The type

of data is the Personal Data described in Annex I. The Data Subjects are the Data Subjects described in Annex I.

2.3. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of ArcPrime as Processor. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.4. ArcPrime shall Process Personal Data received from Customer as a Processor only for the purposes described in the Agreement and as necessary to perform its obligations under the Agreement and strictly in accordance with the documented instructions of Customer except where otherwise required by any Data Protection Laws. As soon as reasonably practicable upon becoming aware, ArcPrime shall inform Customer if, in ArcPrime's opinion, any instructions provided by Customer under this Section 2.4 violate any Data Protection Laws.

2.5. ArcPrime agrees and certifies that it shall not collect, use, or retain Personal Data except to perform the obligations of the Agreement and will not "sell" or "share" Personal Data (as the terms "sell" and "share" are defined under the CCPA).

3. International Transfers of Personal Data.

3.1. ArcPrime shall not make international transfers of Personal Data (nor permit Personal Data to be transferred internationally) unless it takes such measures as are necessary to ensure the transfer is in compliance with Data Protection Laws. If ArcPrime transfers Personal Data from the European Economic Area, Switzerland or the United Kingdom to the United States or any other country that has not been deemed to provide an adequate level of protection, the Standard Contractual Clauses will apply to such transfers.

3.2. With respect to Personal Data transferred from the European Economic Area, the EU SCCs will apply and form part of this DPA, unless the European Commission issues updates to the EU SCCs, in which case the updated EU SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the EU SCCs. For purposes of the EU SCCs, they will be deemed completed as follows:

a. Where Customer acts as a Controller and ArcPrime acts as a Processor, Module 2 applies.
b. Where Customer acts as a Processor and ArcPrime acts as a Subprocessor, Module 3 applies.
c. Clause 7 (the optional docking clause) is not included.
d. Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization).
e. Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body is inapplicable.
f. Under Clause 17 (Governing law), the parties select Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of Ireland.
g. Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.
h. Annexes I, II and III of the EU SCCs are set forth below.
i. By entering into this DPA, the parties are deemed to be signing the EU SCCs.

3.3. With respect to Personal Data transferred from the United Kingdom for which the law of the United Kingdom (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs form part of this DPA and take precedence over the rest of this DPA as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs, in which case the updated UK SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the UK SCCs. The UK SCCs will be deemed completed as follows:

a. Table 1 of the UK SCCs:
    i. The parties' details are the parties set forth in Annex I.
    ii. The Key Contact is the contact set forth in Annex I.
b. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 are the EU SCCs as executed by the parties pursuant to Section 3.2 of this DPA.
c. Table 3 of the UK SCCs: Annex 1A, 1B, and II are as set forth in Annex I and II to this DPA.
d. Table 4 of the UK SCCs: Either party may terminate as set forth in Section 19 of the UK SCCs.
e. By entering into this DPA, the parties are deemed to be signing the UK SCCs and their applicable Tables and Appendix Information.

3.4. With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the EU SCCs will apply and will be deemed to have the following differences to the extent required by the Swiss Federal Act on Data Protection ("FADP"):

a. References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.
b. The term "member state" in the EU SCCs will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.
c. References to Personal Data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.
d. Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

4. **Third Party Requests and Confidentiality**. ArcPrime shall not disclose Personal Data to any individual or to a third party other than: (i) at the request of Customer; (ii) as provided in this DPA; (iii) as necessary to provide the Services; or (iv) as required by applicable law or a valid and binding order of a law enforcement agency. Notwithstanding anything set forth herein, ArcPrime shall ensure that any person that it authorizes to Process the Personal Data shall be subject to a strict duty of confidentiality, and shall not permit any person to Process the Personal Data who is not under such a duty of confidentiality. Except as otherwise required by law, ArcPrime shall promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("Demand") that it receives and which relates to the Personal Data unless prevent from doing so by law. At Customer request, ArcPrime will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner.

5. **Data Subjects' Rights.** For the term of this DPA, ArcPrime shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer, without cost, to enable Customer to respond to any request from a Data Subject to exercise any of its rights under the Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable). In the event that any request from a Data Subject is made directly to ArcPrime, ArcPrime shall promptly inform Customer and provide the full details of the request to Customer.

6. **Technical and Organizational Security Measures**. ArcPrime's technical and organizational security measures are described in Annex II.

7. **Security Incident Notification**. In the event of any Security Incident, ArcPrime will notify Customer without undue delay (but no later than 48 hours) after ArcPrime becomes aware of the Security Incident. In addition, ArcPrime will investigate the Security Incident and provide Customer with

detailed information about the Security Incident in order for Customer to comply with any data breach notification requirements under the Data Protection Law. ArcPrime will also take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

8. Audit and Records.

8.1. ArcPrime shall permit Customer (or its appointed third party auditors) to audit ArcPrime's compliance with this DPA, and shall make available to Customer all information, systems and staff necessary for Customer (or its third party auditors) to conduct such audit. ArcPrime acknowledges that Customer (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that Customer gives ArcPrime reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to ArcPrime's operations. Any onsite audit will be subject to agreement between the parties as to reasonable scope, time, duration, place and conditions for the audit, including compliance with ArcPrime's security protocols. Customer will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Customer believes a further audit is necessary due to a Security Incident suffered by ArcPrime.

8.2. ArcPrime will keep a record of any Processing of Personal Data it carries out on behalf of Customer, which it shall make available to the relevant supervisory authority on request and which shall include:

a. the name and contact details of ArcPrime, ArcPrime's representative and its data protection officer;
b. the categories of Processing carried out on behalf of Customer;
c. transfers of Personal Data to a third country or international organization and the basis on which those transfers are compliant; and
d. a description of data security compliance measures taken by ArcPrime.

9. **Subprocessors.** Customer acknowledges and agrees that ArcPrime may use the subprocessors identified in Annex III ("**Subprocessors**") to provide the Services and provides a general authorization to ArcPrime to use Subprocessors. ArcPrime shall inform Customer of any intended changes regarding ArcPrime's use of Subprocessors and give Customer an opportunity to object. Customer will have fifteen (15) business days from receipt of such notice to notify ArcPrime of its objection to such Subprocessor (providing specific details of the objection), and ArcPrime and Customer will thereafter have a commercially reasonable period of time to cooperate in good faith to address the objection. If ArcPrime is unable to address the objection to Customer's reasonable satisfaction, then Customer may terminate the Agreement. ArcPrime shall impose the same data protection obligations as set forth in this DPA on any Subprocessor prior to the Subprocessor Processing Personal Data. ArcPrime remains responsible for its Subprocessors and liable for their acts and omissions as for its own acts and omissions and any references to ArcPrime's obligations, acts and omissions in this DPA shall be construed as referring also to ArcPrime's Subprocessors.

10. **Data Protection Impact Assessment and Prior Consultation.** Upon Customer's request, ArcPrime shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities, which Customer reasonably considers to be required of Customer by Article 35 or 36 of the EU Data Protection Law, in each case solely in relation to Processing of Personal Data by and taking into account the nature of the Processing and information available to ArcPrime.

11. **Termination**. This DPA shall continue in full force until the expiration or termination of the Agreement or until ArcPrime is no longer Processing any Personal Data of Customer.

12. **Deletion or return of Personal Data.** Upon Customer's request, ArcPrime shall destroy or return to Customer all Personal Data in its possession or control; provided, however, that this requirement

shall not apply to the extent that ArcPrime is required by any EU (or any EU Member State) law to retain some or all of the Personal Data.

13. **Miscellaneous.** The parties will treat the terms and conditions of this DPA as confidential and shall not disclose them to any third party except for Customer's and ArcPrime's auditors or consultants that need access to this information for the purpose of this business relationship as articulated in this DPA and the Agreement. If there is a conflict between any provision in this DPA and any provision in the Agreement, this DPA shall control with regard to the subject matter of this DPA. Except for changes made by this DPA, the Agreement remains unchanged and in full force and effect. Any limitation of liability terms in the Agreement shall apply equally to a party's liability under this DPA; except that no limitation of liability shall apply to (i) the rights of data subjects under Article 82 of the EU Data Protection Law or (ii) a party's liability with respect to breach of applicable Data Protection Laws. This DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Agreement, and each of the parties agrees to submit to the choice of jurisdiction as stipulated in the Agreement with respect to any claim or matter arising under this DPA. If any provision in this DPA is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith. In case of conflict, the order of precedence in respect of the Processing of Personal Data shall be: this DPA and then the Agreement. If the Standard Contractual Clauses are an integral part of this DPA, then the Standard Contractual Clauses shall prevail. This DPA supersedes and replaces all previous written and oral agreements, communications and other understandings relating to the subject matter of this DPA. This DPA may be executed in one or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. Execution of this DPA shall be deemed to be execution of the Standard Contractual Clauses attached hereto.

IN WITNESS WHEREOF, the authorized representative of each party has signed this DPA as of the Effective Date.

ArcIP, Inc.	**Customer**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

ANNEX I

A. LIST OF PARTIES

Name of the Data Exporter: _____

Address: _____

Tel.: n/a; fax: n/a; e-mail: _____

Key Contact: _____

Activities relevant to the data transferred under these Clauses:

Processing as part of the Services ordered by Data Exporter pursuant to a Services Agreement.

Signature and date: This Annex I will be deemed executed upon the date of execution of the DPA to which it is attached.

Role: Controller

Name of the Data Importer: ArcIP, Inc.

Mailing Address: 632 True Wind Way, Unit 609, Redwood City, California 94063 US

Tel.:(408) 8382110 fax: n/a; e-mail: info@arcprime.com

Key Contact: Jonathan Liu, jon@arcprime.com

Activities relevant to the data transferred under these Clauses:

Processing as part of the Services ordered by Data Exporter pursuant to a Services Agreement.

Signature and date: This Annex I will be deemed executed upon the date of execution of the DPA to which it is attached.

Role: Processor

B. DESCRIPTION OF TRANSFER

Data Importer is engaged in providing Services relating to leveraging a comprehensive database of startups and professionals.

Categories of data subjects whose personal data is transferred: user information and client lists.

Categories of personal data transferred: Personal Data provided by the Data Exporter to the Data Importer in connection with its use of the Services. Such Personal Data may include names and contact information.

Sensitive data transferred: Not applicable.

Frequency of the transfer: Ongoing during the provision of the Services.

Nature of the processing: To the extent necessary to provide the Services.

Purposes of the data transfer: To provide the Services to the Data Exporter.

The period for which the personal data will be retained: For the duration of the Services Agreement with the Data Exporter and for such longer period as may be required to comply with applicable laws.

Transfers to sub-processors: See Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be the Data Protection Commission of Ireland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

ArcPrime has implemented and shall maintain a security program that includes appropriate administrative, physical, and technical safeguards designed to protect Personal Data from data breaches and to help ensure the ongoing confidentiality, integrity, and availability of the Personal Data and Processing systems, taking into account the nature of the Personal Data that ArcPrime processes and the risks involved.

The following sections describe ArcPrime's current technical and organizational measures with respect to data security. ArcPrime may change these measures at any time without notice, provided it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

ArcPrime is SOC2 Type 2 & ISO 27001 compliant.

Product Security

- Authentication measures, including secure methods of assigning, selecting, and storing access credentials, measures designed to restrict access to active users.
- Setting of customer access permission levels globally or within specific departments appropriate to the level of access required.

System Security

- Use of managed infrastructure services that are globally recognized for their robust security protocols.
- Encryption of data in transit using the industry standard for HTTPS security (TLS 1.2 and TLS 1.3) so that requests are protected from eavesdroppers and man-in-the-middle attacks.
- Encryption of persistent data at rest using industry-standard AES-256 algorithms.
- SSL certificates.
- Appropriate monitoring systems and other technical security measures intended to prevent and detect security breaches such as firewall protection, antivirus protection, security patch management, logging of access to or disclosure of personal information, and intrusion detection.

Physical Security

- Use of world-class data hosting centers that use state-of-the-art multilayer access, alerting, and auditing measures.
- Physical security to safeguard facilities and records containing personal information from unauthorized physical access, tampering or theft, including facility access controls.

Operational Security

- Secure access controls, including measures designed to limit access to personal information based on need-to-know, supported by appropriate policies, procedures and controls to facilitate access authorization, establishment, modification, and termination.
- Employee training and awareness programs designed to ensure workforce members are aware of and adhere to ArcPrime's security procedures and practices.
- Frequent updating of security policies to be consistent with best certificate standards.
- Employee computers are equipped with monitoring that enforce ArcPrime's security policies, including administrative access, screen lockout, strong passwords, encrypted disks, and virus scanners.
- Employee access to secure environments is enforced using Google account infrastructure to verify employee account identity and require two-factor authentication for apps that access critical infrastructure or customer data.
- Access to administrative interfaces additionally enforce administrator permissions where applicable, and all administrative access is logged and auditable both in the form of traditional web server logs

and session recordings to make it easy to find and review any administrative activities with full fidelity.
- All changes to source code are subject to automated testing and any that affect security require pre-commit code review by a qualified engineering.
- All code is deployed to a staging environment for quality assurance and automated tests must pass prior to updating production services.
- Data back-up and disaster recovery procedures intended to permit continued provision of service in an emergency or disaster, including highly redundant datastores, rapid recovery infrastructure, and point-in-time backups.
- Periodic assessment of threats and vulnerabilities to personal information and the effectiveness of the security procedures and practices implemented to comply with Data Protection Laws and Regulations.
- Selection of processors includes security due diligence.
- Employee contracts include a confidentiality agreement.

Application Security

- Servers use managed infrastructure that utilizes firewalls to restrict system access from external and internal networks, DDoS mitigation, spoofing and sniffing protections, and port scanning.
- Request-handling code paths have frequent user re-authorization checks, payload size restrictions, rate limiting where appropriate, and other request verification techniques.
- All requests are logged and searchable by operations staff.
- Client code utilizes multiple techniques to ensure that using the ArcPrime app is safe and that requests are authentic, including XSS and CSRF protection, signed and encrypted user authentication cookies, and session expiration.
- Third party security is engaged to perform penetration tests on the ArcPrime app.
- Access to the ArcPrime RPC API endpoints requires an access key.
- Integrations with other apps are all opt-in and authenticated via OAuth or other applicable mechanisms required by the third party app.
- ArcPrime uses a well-recognized Level 1 PCI payment processor.

Incident Reporting

- Written protocol for handling security events, including escalation procedures, rapid mitigation, and post-mortem.
- All employees are informed of ArcPrime's incident reporting requirements and their duties with respect to responding to a security event.
- Maintenance of a Responsible Disclosure Policy that encourages reporting of any security vulnerability in ArcPrime's service.

ANNEX III

LIST OF SUB-PROCESSORS

NAME	ADDRESS	CONTACT PERSON	DESCRIPTION OF PROCESSING
Supabase	548 Market St, San Francisco, CA 94104	https://supabase.com/support	Cloud data processing and warehousing
Google Cloud Platform	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	https://cloud.google.com/support	Cloud data processing and warehousing
Microsoft Corporation (Azure OpenAI Service)	One Microsoft Way, Redmond, WA 98052, USA	https://azure.microsoft.com/support	Large language model inference