DATA PROCESSING ADDENDUM

(Last Updated: May 30, 2023)

This is a reference copy of the Arcadia Data Processing Addendum (DPA), which may be required for some Arcadia customers. To sign the DPA, please reach out to your Arcadia sales representative.

This Data Processing Addendum ("**Addendum**") forms part of the agreement between Client (as defined below) and Arcadia (as defined below) for Services (as defined below) (collectively, the "Agreement"). This Addendum shall apply when Arcadia Processes Personal Data disclosed to it by Client. Upon mutual execution, this Addendum is incorporated into the Agreement. This Addendum applies where and only to the extent that Client acts as a business or the controller (as applicable) with respect to the processing of Personal Data, and in such event Client has appointed Arcadia to process Personal Data as a processor or service provider (as applicable) on its behalf in connection with the Services. This Addendum is intended to demonstrate the parties' compliance with data protection laws that may be applicable to Arcadia's delivery and Client's receipt of Services (together "**Data Protection Laws**").

1. Defined Terms. Any capitalized terms not defined herein shall have the meanings given in the Agreement. For purposes of this Addendum, words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in the applicable Data Protection Laws. In particular:

(a) "**CCPA**" means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 *et seq*. as may be amended, superseded or replaced.

(b) "**Controller**" has the meaning given to it in the applicable Data Protection Laws.

(c) "**Data Subject**" means "Data Subject" as used by the EEA Data Protection Law or "Consumer" as used by other applicable laws.

(d) "**EEA 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 ("**General Data Protection Regulation**" or "**GDPR**"), and laws implemented by EEA members, which contain derogations from, or exemptions or authorizations for the purposes of, the GDPR, or which are otherwise intended to supplement the GDPR or convert the GDPR into domestic law.

(e) "**EU Standard Contractual Clauses**" or "**Clauses**" means the standard contractual clauses, including Annexes I and II, for the transfer of personal data to third countries pursuant to the GDPR, with optional clauses applied (except for option 1 of Clause 9(a), the optional language in Clause 11(a), and option 2 of Clause 17), as officially published by the European Commission Implementing Decision 2021/914, dated 4 June 2021, and as updated or replaced by the European Commission from time to time.

(f) "**Personal Data**" has the meaning given to it in the applicable Data Protection Laws.

(g) "**Process**" or "**Processing**" has the meaning given to it in the applicable Data Protection Laws.

(h) "**Processor**" has the meaning given to it in the applicable Data Protection Laws.

(i) "**Subprocessor**" means any natural or legal person, public authority, agency or other body which processes personal data on behalf of a Processor (including any affiliate of the Processor).

(j) **United Kingdom Standard Contractual Clauses** ("**UK SCCs**") means the EU SCCs and the UK International Data Transfer Addendum as officially published at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-

gdpr/international-data-transfer-agreement-and-guidance/ with the option of Exporter only for Table 4 and the Alternative Part 2 Mandatory Clauses.

2. Details of Processing. The context for the Processing of the Controller's Personal Data by Arcadia is the performance of Arcadia's obligations under the Agreement, and Arcadia will Process such Personal Data until the expiration or termination of the Agreement unless otherwise instructed in writing by Client. The types of Personal Data, the categories of Data Subjects and other details of the Processing activities are described in Annex I.

3. Subprocessors. Prior to any addition or replacement of engagement of any Subprocessors, Arcadia will update the Subprocessors list at https://vault.pactsafe.io/s/db63018b-ec5f-4792-8bc4-46f3950b6724/legal.html#third-party-subprocessors. Within thirty (30) days after Arcadia's notification of the intended change, Client can object to any new Subprocessor by sending notice to privacy@arcadia.com on the basis that such addition would cause Client to violate applicable legal requirements. If Client objects to Arcadia's use of any new Subprocessor by so giving written notice to Arcadia within thirty (30) days of being informed by Arcadia of the appointment of such new Subprocessor and Arcadia fails to provide a commercially reasonable alternative to avoid the Processing of Personal Data by such Subprocessor within thirty (30) days of Arcadia's receipt of Client's objection, Client may, as its sole and exclusive remedy, terminate any Services that cannot be provided by Arcadia without the use of the objected to new Subprocessor. If Client does not object within such period, the respective Subprocessor may be commissioned to Process Personal Data. Subprocessors are required to abide by the same level of data protection and security as Arcadia under this Addendum as applicable to their Processing of Personal Data and Arcadia will remain responsible to Client for any acts or omissions of any Subprocessor that cause Arcadia to breach any of Arcadia's obligations under this Addendum. Arcadia will restrict the Subprocessors' access to, and Processing of, Personal Data only to what is necessary to provide products or services to Client in accordance with the Agreement.

4. Processing Obligations. In accordance with Data Protection Laws:

(a) Arcadia shall only Process the Personal Data (i) as needed to provide the products or services to Client in accordance with the Agreement, (ii) in accordance with the specific instructions that it has received from Client, including with regard to any transfers, and (iii) as needed to comply with laws that Arcadia is subject to, and in such case, Arcadia will inform Client of that legal requirement before Processing unless the law prohibits such information on important grounds of public interest;

(b) Arcadia shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Arcadia shall implement the measures set forth in Annex II and as set forth in the Agreement to ensure a level of security appropriate to the risks that are presented by Arcadia's Processing of Personal Data, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons;

(d) Taking into account the nature of the Processing, Arcadia shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Controller's obligation to respond to requests for exercising Data Subjects' rights;

(e) Taking into account the nature of Processing and the information available to Arcadia, Arcadia shall assist Client with Client's compliance with its obligations regarding personal data breaches, data protection impact assessments, security of processing, and prior consultation, each as and to the extent required by applicable Data Protection Laws;

(f) Upon Client's written request, Arcadia shall either delete or return to Client all of the Personal Data in Arcadia's possession after the end of the provision of products or services relating to Processing, unless otherwise required by applicable laws. In such cases, Arcadia will ensure that Client Personal Data is only Processed as necessary to comply with applicable laws;

(g) Upon Client's written request, Arcadia shall provide Client with a confidential summary report of its external auditors to verify the adequacy of its security measures and other information necessary to demonstrate Arcadia's compliance with this Addendum and, to the extent required by Data Protection Laws (and no more than once per year unless otherwise required by Data Protection Laws) allow for, and contribute to, audits, including inspections, conducted by Client or another auditor mandated by Client. Client agrees to treat such summary report and other information described in this subsection as Arcadia's Confidential Information under the terms of the Agreement;

(h) Arcadia shall promptly inform Client if, in Arcadia's opinion, an instruction by Client infringes Data Protection Laws; and

(i) Arcadia shall comply with all Data Protection Laws in respect of the Services applicable to Arcadia as Processor. Arcadia is not responsible for determining the requirements of laws or regulations applicable to Client's business, or that a product or service meets the requirements of any such applicable laws or regulations. As between the parties, Client is responsible for the lawfulness of the Processing of the Client Personal Data and for taking appropriate steps in Client's control to maintain appropriate security, protection and deletion of Client Personal Data. If Client is acting as a Processor, Client has obtained the authorisations required from the relevant Controller(s) and Client shall serve as the single point of contact for Arcadia. Client shall not use the Services in a manner that would violate applicable Data Protection Laws.

5. Transfers of Personal Data.

(a) Client acknowledges and agrees that Arcadia may transfer and process Personal Data in the United States and anywhere else in the world where Arcadia, its Affiliates or its Sub-processors maintain data processing operations. Arcadia and Client shall work together to ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this Addendum. To the extent Client's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e. the European Economic Area, the United Kingdom or Switzerland) to a recipient in locations outside of that jurisdiction to a country not providing an adequate level of protection pursuant to the applicable Data Protection Laws ("Non-Adequate Country"), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws on the terms set out in the following sections, which shall apply in such event:

(b) By entering into this Addendum, Client and Arcadia are entering into the EU Standard Contractual Clauses, including Annexes I and II, if Client, Arcadia, or both are located in a Non-Adequate Country. If the EU Standard Contractual Clauses are not required because both parties are located in a country considered adequate by the applicable Data Protection Laws, but during the Agreement the country where Client or Arcadia is located becomes a Non-Adequate Country, then the EU Standard Contractual Clauses will apply to Personal Data that is transferred to such Non-Adequate Country.

(c) The parties acknowledge that the applicable module of the EU Standard Contractual Clauses will be determined by their role as Controller and/or Processor under the circumstances of each case and are responsible for determining the correct role undertaken in order to fulfill the appropriate obligations under the applicable module. When Client is acting as a Controller, module 2 (Controller-to-Processor) of the EU Standard Contractual Clauses will apply to the Personal Data transferred to any Non-Adequate Country, and when Client is acting as a Processor, module 3 (Processor-to-Processor) of the EU Standard Contractual Clauses will apply to the Personal Data transferred to any Non-Adequate Country.

(d) With regards to (i) Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply; (ii) Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 3 (Subprocessing) of this Addendum; (iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply; (iv) in Clause 13 of the EU Standard Contractual Clauses and as set forth in Annex I.C below, the competent supervisory authority with responsibility for ensuring compliance with the GDPR as regards the Personal Data transferred under the EU Standard Contractual Clauses shall be the Data Protection Commission of Ireland; (v) in Clause 17 of the EU Standard Contractual Clauses, the parties agree that the EU Standard Contractual Clauses shall be governed by the laws of Ireland. With regards to Clause 18(b) of the EU Standard Contractual Clauses, the parties agree that the courts of Dublin, Ireland, shall resolve any dispute. Annex I and Annex II of the EU Standard Contractual Clauses shall be completed with the information set out in Annex I and II to this DPA.

(e) 5.3 Regarding UK SCCs, if Arcadia is not established in an Adequate Country: Arcadia is hereby entering into UK SCCs as a Data Importer with Client and in so doing, Arcadia is hereby entering into the EU SCCs on the terms set out in Section 5© above subject to the amendments in the UK International Data Transfer Addendum.

6. Personal Data Breach. Arcadia will promptly investigate all allegations of unauthorized access to, or use or disclosure of the Personal Data. If Arcadia reasonably believes there has been a Personal Data breach, Arcadia will notify Client without undue delay and in any event within forty-eight (48) hours, and provide sufficient information to allow Client to report the personal data breach or notify Data Subjects as required by applicable Data Protection Laws.

7. Records. Arcadia shall maintain all records required by applicable Data Protection Laws, and (to the extent they are applicable to

Arcadia's activities for Client) Arcadia shall make them available to Client upon its written request.

8. Third Party Requests. If any government or regulatory authority requests access to Personal Data, unless prohibited by law, Arcadia will notify Client of such request to enable Client to take necessary actions to communicate directly with the relevant authority and respond to such request. If Arcadia is prohibited by law to notify Client of such request, it will use reasonable efforts to challenge the prohibition on notification and will provide the minimum amount of information permissible when responding, based on a reasonable interpretation of the request

9. California. To the extent the Personal Data is subject to the CCPA, the parties agree that Client is a business and that it appoints Arcadia as its service provider to process Personal Data as permitted under the Agreement (including this Addendum) and the CCPA, or for purposes otherwise agreed in writing (the "Permitted Purposes"). Client and Arcadia agree that: (a) Arcadia shall not retain, use or disclose personal information for any purpose other than the Permitted Purposes; (b) Personal Data was not sold to Arcadia and Arcadia shall not "sell" personal information (as defined by the CCPA); (c) Arcadia shall not retain, use or disclose personal information outside of the direct business relationship between Arcadia and Client.

10. Entire Agreement; Order of Precedence; No Conflict. Except as amended by this Addendum, the Agreement will remain in full force and effect. Client agrees that this Addendum, including any claims arising from them, are subject to the terms set forth in the Agreement, including the limitations of liability. If there is any conflict or inconsistency between the EU Standard Contractual Clauses, the Addendum and/or the remainder of the Agreement, then the following order of precedence will apply: the EU Standard Contractual Clauses (if applicable), the remainder of this Addendum and the remainder of the Agreement. Nothing in this Addendum is intended to modify or contradict the applicable terms in the Data Protection Laws or the EU Standard Contractual Clauses or prejudice the fundamental rights or freedoms of Data Subjects under Data Protection Laws.

ANNEX 1 TO EXHIBIT B, DATA PROCESSING ADDENDUM

A. List of Parties

1. Data Exporter(s)

Name: The data exporter is Client.

Address: As set out in the Agreement.

Contact person's name, position and contact details: As set out in the Agreement or as otherwise notified in writing to Arcadia by Client.

Activities relevant to the data transferred under these Clauses: As set out in the Agreement.

Signature and date: By entering into the Agreement, Client is entering into these Clauses and deemed to have signed this Annex I on the effective date of the Agreement.

Role (controller/processor): Client is Controller or Processor or both. The role of Client as Controller, Processor, or both is determined by the circumstances of each case and Client is responsible for determining the correct role undertaken in order to fulfil the appropriate obligations under the applicable module.

2. Data Importer(s)

Name: The data importer is Arcadia acting as a Processor or Subprocessor, as applicable, if located in a Non-Adequate Country.

Address: As set out in the Agreement.

Contact person's name, position and contact details: As set out in the Agreement.

Activities relevant to the data transferred under these Clauses: As set out in the Agreement.

Signature and date: By entering into the Agreement, Arcadia is entering into these Clauses in such cases where Arcadia is located in a Non-Adequate Country and deemed to have signed this Annex I on the effective date of the Agreement.

Role (controller/processor): Arcadia as Processor.

B. Description of Transfer

1. Categories of Data Subjects whose Personal Data is transferred

Data exporter may submit Personal Data to data importer the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Employees of data exporter
- Data exporter's users authorized by data exporter to use the Services
- Employees or contact persons of data exporter's customers, business partners and vendors

2. Categories of Personal Data transferred

Data exporter may submit Personal Data to Processor the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Employment information (such as title, position, employer)
- Contact information (such as email, phone, physical address)
- IP address, online identifier or other ID data

Utility credential and endpoint data - Personal Data that might be included in utility endpoint data is generally limited to service addresses along with other non-Personal Data such as utility financial and operational data, services areas, baseline areas (territories), services offered, tariff rate plans, incentives, and rebates, definitions of seasons, calendars and times of use; definitions of billing demand formulas and other quantities; typical usage and cost profiles; and typical building usage and cost.

3. Special or sensitive categories of Personal Data transferred

None

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

Personal Data is transferred in accordance with Client's instructions and at Client's determination, but it is generally on a continuous basis.

5. Nature of the Processing

The Personal Data transferred may be subject to the following Processing activities: collecting, monitoring, supporting, operations, storing, hosting, backup, development and the other services as set forth in the Agreement.

6. Purposes(s) of the data transfer and further processing

The transfer and Processing of Personal Data is made for the following purposes: To provide the Services and support as set forth in the Agreement.

7. Duration of Processing

The Processing of Personal Data will occur until the expiration or termination of the Agreement unless otherwise instructed in writing by the Client.

8. Transfers to Subprocessors

The subject matter, nature and duration of Processing are as set forth in the above sections.

C. Competent Supervisory Authority

The competent supervisory authority for Arcadia is the Data Protection Commission of Ireland in accordance with Clause 13 of the EU Standard Contractual Clauses.

D. Arcadia Privacy Contact

The Arcadia privacy contact can be contacted at privacy@arcadia.com.

ANNEX 2 TO APPENDIX B, DATA PROCESSING ADDENDUM

Technical and Organizational Security Measures

1. **Security.** Arcadia shall, during the term of the Agreement, comply in all material respects with the following technical and organizational security measures applicable to the Services:
    a. **General.**
        i. All Arcadia applications that are accessible from the Internet or process personal data are approved prior to launch or implementation by Arcadia's information security.
    b. **Physical Security.**
        i. The equipment hosting the Arcadia Offerings is located in a physically secure facility, which requires badge access at a minimum.
        ii. Physical access to infrastructure housing the Arcadia Offerings is restricted and access allowed based on a need-to-know basis.
        iii. Electronic media (online or offline) and confidential hard copy material is appropriately protected from theft or loss.
    c. **Authentication.**
        i. All access to Arcadia systems is controlled by an authentication method involving a minimum of a unique user ID/complex password combination
        ii. Privileged users and administrators use strong authentication.
        iii. Passwords are never stored in clear text.
        iv. Passwords are complex and not easy to guess or crack. Effectiveness of authentication is tested on a regular basis to verify that unauthorized authentication is not easily permitted.
        v. Remote network access is secured by two-factor authentication.
        vi. All activity performed under a User ID is the responsibility of the individual assigned to that user ID. Users do not share their User ID/password with others or allow other employees to use their User ID/password to perform actions.
        vii. Use of generic user account is not permitted.
    d. **Authorization.**
        i. Logical or network access to infrastructure housing the Services is restricted and access allowed based on a need-to-know basis.

ii. Access requests are documented and approved based on a business need utilizing the principle of least privilege.

iii. Access rights are reviewed on a periodic basis.

iv. Upon termination or resignation of personnel, access is revoked in a timely manner.

e. **Change Management.** Change requests are documented via a ticketing system. The change request contains, at a minimum, the following information.

i. Business justification for the change

ii. Nature of defect (if applicable)/enhancement

iii. Testing required

iv. Back-out procedures

v. Systems affected

vi. User contact

vii. The process to review and approve change requests must be documented. The process must include management approval.

f. **Network Security.**

i. Industry standard firewalls are implemented to protect the application environment and associated data from the Internet and untrusted networks.

ii. Inbound and outbound connections are denied unless expressly allowed.

iii. Firewall events are monitored in order to detect potential security events.

iv. Network Intrusion Detection or Prevention Systems (NIDS/NIPS) are implemented to monitor traffic for applications handling confidential information.

v. Effectiveness of controls are tested on a periodic basis.

g. **Logging and Monitoring.** Security relevant events, including, but not limited to, login failures, use of privileged accounts, changes to access models or file permissions, modification to installed software, or the operating system, changes to user permissions, or privileges or use of any privileged system function, are logged on all systems.

h. **System Security.**

i. Systems are securely configured according to a security baseline. This baseline includes removing unnecessary services and changing default, vendor-supplied or otherwise weak user accounts and passwords.

ii. System components maintain current security patch levels.

iii. Web servers are hardened according to a secure baseline.

iv. Web servers are configured to accept requests for only authorized and published directories. Default sites, executable or directory listings are disabled.

v. An inventory of technology used to store or process Client data is maintained.

i. **Security Awareness.** Arcadia will design and maintain a Security Awareness program that will train employees upon hire and annually afterwards maintain regular touchpoints with employees on emerging

threats.

j. **Device and Media Control.**

   i. Arcadia will maintain a device management platform ensuring endpoint controls (e.g. antivirus/antimalware, disk encryption, patching) are applied uniformly to user endpoints.

   ii. Arcadia will encrypt Client data utilizing at minimum TLS 1.2 in transit and AES-256 at rest.

   iii. Arcadia will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with Industry Best Practices for media sanitization.

2. **Viruses and Disabling Code**. Arcadia will use commercially reasonable efforts to avoid introducing any viruses, time or logic bombs, Trojan horses, worms, timers, clocks, trap doors, or other computer instructions, devices, or techniques that erase data or programming, infect, disrupt, damage, disable, or shut down the Services, including, without limitation, its security or data. In the event a virus or similar item is found to have been introduced into Arcadia's system, Arcadia will: (a) use commercially reasonable efforts to reduce or eliminate the effects of the virus or similar item; and (b) if the virus or similar item causes a loss of operational efficiency or loss of data, mitigate and restore.

3. **Incident Reporting/Investigation.** Arcadia shall notify Client of any confirmed security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client data ("Data Breach") without undue delay , unless otherwise prohibited by state or federal law. Arcadia will provide Client with regular updates with any new details regarding the Data Breach. A report about the Data Breach will be provided to Client as soon as reasonably practicable and after considering appropriate precautions or limitations such as attorney-client privilege.

4. **Investigations.** Upon written notice to Arcadia, Arcadia shall assist and support Client in the event of an investigation by any regulator, including a data protection regulator, or similar authority, if and to the extent that such investigation relates to personal data handled by Arcadia on behalf of Client. Such assistance shall be at Client's sole expense, except where such investigation was required due to Arcadia's gross negligence.

5. **Audit**. Arcadia will periodically review control effectiveness and remediate any deficiencies identified.