**GDPR DATA PROTECTION ADDENDUM**

This Data Protection Addendum ("**DPA**") to the Master Services Agreement (the “**MSA**” or “**Agreement**”) (as defined below) is entered into by and between **Arcadia University**, (who may also be identified in this DPA as **“Client,”** **“Controller,”** or **“Exporter”**) and **[VENDOR]** (who may also be identified in this DPA as **“Vendor,” “Processor,”** or **“Importer”**), each a "**Party**" and collectively the "**Parties.**"

Capitalized terms in this DPA, not otherwise defined in this Addendum or in the MSA (as defined below) shall have the meaning ascribed to them in applicable data protection laws, including but not limited to, the European Union General Data Protection Legislation (hereinafter the “GDPR”) and the United Kingdom Data Protection Act 2018, 2018 c. 12 (hereinafter the “UK Data Protection Act”).

**PREAMBLE**

**Whereas,** Vendor and Arcadia have entered into an agreement whereby Vendor will provide services to Arcadia;

**Whereas,** Arcadia is a University based in the United States with student, offices, employees and agents located in the European Union (EU), European Economic Area (EEA), and/or the United Kingdom (UK);

**Whereas,** Under the terms of the MSA, Vendor may carry out data processing activities on behalf of Arcadia in relation to Personal Data of individuals located in the EU/EEA and/or UK, to which activities the GDPR or UK Data Protection Act may apply;

**Whereas,** For the purposes of this DPA, Arcadia is considered a “Data Controller” and Vendor is considered a “Data Processor,” as defined by the GDPR and UK Data Protection Act;

**Whereas,** The Parties have agreed in those cases where Vendor or any of its affiliates which Process Personal Data on Arcadia’s behalf is established outside the EU/EEA or UK or in a country which does not ensure an adequate level of data protection by a European Commission Decision pursuant to the GDPR or UK Data Protection Act, to enter into the appropriate standard contractual clauses to secure the international transfer of Personal Data;

**Whereas**, Therefore, the Parties mutually agree to execute this DPA in order to meet the European Union and United Kingdom privacy law requirements, as applicable, by adopting the substantial contents of the **EU Model Clauses for Processors** and the **UK Model Clauses for Processors**.

**Whereas,** For this purpose, the present DPA sets forth the terms that follow and contains the following Attachments and Annexes:

|  |  |
| --- | --- |
| * Attachment 1
 | * Contains the details of the Parties, data subjects, categories of data, and processing operations covered by this Addendum as required for the adoption of Standard Contractual Clauses (as defined below);
 |
| * Attachment 2
 | * Contains a description of the technical and organisational security measures implemented by the data importer as required for the adoption of Standard Contractual Clauses (as defined below);
 |
| * [Annex A](https://drive.google.com/file/d/1yXkP7bvWRCrvwk1bwa0Hdu9Igi2vOa7p/view?usp=sharing)
 | * Contains the contractual clauses set out in the European Commission’s Implementing Decision (EU) 2021/914 of 4th June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries, adopted by the Parties as their own contractual clauses where applicable, and as modified by Attachments 1 and 2;
 |
| * [Annex B](https://drive.google.com/file/d/1shJk1-RI3kQzSBnfrlb1F5LqBdmL3wvq/view?usp=sharing)
 | * Contains the contractual clauses set forth by the UK pursuant to the UK Data Protection Act and the Data Protection, Privacy and Electronic Communications Regulations 2019, 2019 No. 419, adopted by the Parties as their own contractual clauses where applicable, and as modified by Attachments 1 and 2;
 |

NOW THEREFORE, in consideration of the mutual obligations set out herein, and intending to be legally bound, the parties hereby agree to the terms and conditions set out below.

# **Definitions**

## In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

### “**Applicable Laws**” means any applicable federal, state, and/or international law in respect of which Arcadia and/or Vendor is subject, including, to the extent applicable, the European Union’s General Data Protection Regulation 2016/679 (“**GDPR**”), laws implementing or supplementing the GDPR, the United Kingdom Data Protection Act of 2018, 2018 c 12 (“**UK Data Protection Act**”), and the data protection or privacy laws of other countries;

### “**Arcadia Data**” means any Personal Data Processed by Vendor on behalf of Arcadia pursuant to or in connection with the Agreement.

###  “**Data Subject**” means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

### “**Personal Data**” means any information relating to a Data Subject;

### “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed;

### “**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;

### “**Restricted Transfer**”means:

#### a transfer of Arcadia Data between Arcadia and Vendor; or

#### an onward transfer of Arcadia Data between Vendor and a Subprocessor or between two establishments of Vendor or a Subprocessor,

### in each case, where such transfer would cause Arcadia Data to be transferred to any jurisdiction outside the United Kingdom, the European Union, or the European Economic Area for which the applicable regulatory body has not adopted an adequacy decision or adequacy regulation;

### “**Services**” means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Arcadia pursuant to the Agreement;

### “**Standard Contractual Clauses**” means the contractual clauses set out in the European Commission’s Implementing Decision (EU) 2021/914 of 4th June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries or the contractual clauses set forth by the UK pursuant to the UK Data Protection Act and the Data Protection, Privacy and Electronic Communications Regulations 2019, 2019 No. 419, as applicable;

### “**Subprocessor**” means any person or entity appointed by or on behalf of Vendor to Process Personal Data on behalf of Arcadia in connection with the Agreement; and

## The word “**include**” shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

# **Processing of Arcadia Data**

## Arcadia shall determine the purpose and means of Vendor’s Processing of Arcadia Data.

## Vendor shall:

### comply with all Applicable Laws in the Processing of Arcadia Data;

### use Arcadia Data only for the purpose of fulfilling its respective duties and providing Services under the Agreement; and

### not otherwise Process Arcadia Data other than on Arcadia’s documented instructions unless Processing is required by Applicable Laws to which Vendor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Arcadia of that legal requirement before the relevant Processing of that Personal Data.

## Arcadia instructs Vendor (and authorizes Vendor to instruct each Subprocessor) to:

### Process Arcadia Data; and

### in particular, transfer Arcadia Data to any country or territory,

### as reasonably necessary for the provision of the Services and consistent with the Agreement.

## Vendor shall immediately notify Arcadia of any changes in relation to the Processing that are likely to result in a high risk to the rights and freedoms of natural persons.

## Attachment 1 to this Addendum sets out certain information regarding Vendor’s Processing of the Arcadia Data. Arcadia may make reasonable amendments to Attachment 1 by written notice to Vendor from time to time as Arcadia reasonably considers necessary to meet those requirements.

# **Vendor Personnel**

## Vendor shall take reasonable steps to ensure the reliability of any employee, agent, or contractor who may have access to the Arcadia Data, ensuring in each case that access is strictly limited to those individuals who need to know and/or access Arcadia Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual’s duties, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

# **Security**

## 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, Vendor shall in relation to the Arcadia Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk (“**Data Security Standards**”), including, as appropriate:

### the pseudonymisation and encryption of Arcadia Data;

### the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

### the ability to restore the availability and access to Arcadia Data in a timely manner in the event of a physical or technical incident; and

### a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

## Without prejudice to the generality of the foregoing, the Data Security Standards that Vendor shall implement and maintain are as follows:

### DATA SECURITY GOVERNANCE. Vendor maintains internal organizational and governance procedures to appropriately manage information throughout its lifecycle. Vendor regularly tests, assesses and evaluates the effectiveness of its Data Security Standards.

### PHYSICAL ACCESS CONTROL. Vendor uses a variety of measures appropriate to the function of the location to prevent unauthorized access to the physical premises where Arcadia Data is processed. Those measures include:

#### Centralized key and code management, card-key procedures

#### Batch card systems including appropriate logging and alerting mechanisms

#### Surveillance systems including alarms and, as appropriate, CCTV monitoring

#### Receptionists and visitor policies

#### Locking of server racks and secured equipment rooms within data centers

### VIRTUAL ACCESS CONTROL. Vendor implements appropriate measures to prevent its systems from being used by unauthorized persons. This is accomplished by:

#### Individual, identifiable and role-based user account assignments; role-based and password protected access and authorization procedures

#### Centralized, standardized password management and password policies (minimum length/characters)

#### User accounts are disabled after excessive failed log-on attempts

#### Automatic log-off in case of inactivity

#### Anti-virus management

#### Firewall management

### DATA ACCESS CONTROL. Individuals that are granted use of Vendor systems are only able to access the data that are required to be accessed by them within the scope of their responsibilities and to the extent covered by their respective access permission (authorization) and such data cannot be read, copied, modified or removed without specific authorization. This is accomplished by:

#### Authentication at operating system level

#### Separate authentication at application level and/or authentication against centrally managed authentication system

#### Change control procedures that govern the handling of changes (application or OS) within the environment

#### Remote access has appropriate authorization and authentication

#### Logging of system and network activities to produce an audit-trail in the event of system misuse

#### Implementation of appropriate protection measures for stored data commensurate to risk, including encryption, pseudonymisation and password controls

### DISCLOSURE CONTROL. Vendor implements appropriate measures to prevent data from being read, copied, altered or deleted by unauthorized persons during electronic transmission and during the transport of data storage media. Vendor also implements appropriate measures to verify to which entities’ data are transferred. This is accomplished by:

#### Data transfer protocols including encryption for data carrier/media

#### Profile set-up data transfer via secure file transfer methods

#### Encrypted VPN

#### No non-secure physical transfers of backup media

### DATA ENTRY CONTROL. Vendor implements appropriate measures to monitor whether data have been entered, changed or removed (deleted), and by whom. This is accomplished by:

#### Documentation of administration activities (user account setup, change management, access and authorization procedures)

#### Archiving of password-reset and access requests

#### System log-files enabled by default

#### Storage of audit logs for audit trail analysis

#### Centralization of audit logs to correlate incidents cross-system

### INSTRUCTIONAL CONTROL. Vendor implements appropriate measures to ensure that data may only be processed in accordance with Arcadia’s instructions. Those measures include:

#### Binding policies and procedures on Vendor employees

#### Where Subprocessors are engaged in the processing of data, including appropriate contractual provisions to the agreements with Subprocessors to maintain instructional control rights

### AVAILABILITY CONTROL. Vendor maintains appropriate levels of redundancy and fault tolerance for accidental destruction or loss of data, including:

#### Extensive and comprehensive backup and recovery management systems that backup Arcadia Data at reasonably regular intervals

#### Documented disaster recovery and business continuity plans and systems

#### Storage and archive policies

#### Anti-virus, anti-spam and firewall systems and management including policies

#### Data centers are appropriately equipped according to risk, including physically separated back up data centers, uninterruptible power supplies (including backup generators), fail redundant hardware and network systems and alarm and security systems (smoke, fire, water)

#### Hard disk redundancy is used in all systems, in both local storage and SAN-based storage environments

#### All critical systems have backup and redundancy built into the environment

### SEPARATION CONTROL. Vendor implements appropriate measures to ensure that data that are intended for different purposes are processed separately. This is accomplished by:

#### Access request and authorization processes provide logical data separation

#### Separation of functions (production / testing)

#### Segregation of duties and authorizations between users, administrators and system developers

### Vendor warrants that it has implemented the above Data Security Standards and that it will maintain such Data Security Standards during the term hereof. Vendor shall ensure by means of appropriate protective mechanisms that access to Arcadia Data is strictly limited to those employees of Vendor who require access in order to fulfill Vendor’s obligations under the Agreement.

### Acknowledging that the Data Security Standards are subject to technical progress and development, the parties agree that Vendor shall be authorized to implement adequate alternative technical and organizational measures provided, however, that (i) such measures shall not materially fall short of the level of security provided by the Data Security Standards; (ii) comply with the requirements under Applicable Laws; and (iii) are in line with state of the art data security standards. Vendor shall immediately notify Arcadia of any material changes to the Data Security Standards. Vendor shall regularly test and audit the Data Security Standards for adequateness and compliance with Applicable Laws and immediately take any corrective action required.

# **Subprocessing**

## Arcadia authorises Vendor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Agreement.

## The Subprocessors for the Services used by Vendor are identified in Attachment 1 to this DPA. Vendor may continue to use those Subprocessors, identified in Attachment 1, already engaged by Vendor as of the date of this Addendum, subject to Vendor in each case as soon as practicable meeting the obligations set out in section 5.4.

## Vendor shall give Arcadia prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within thirty (30) days of receipt of that notice, Arcadia notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment then Vendor shall not appoint (nor disclose Arcadia Data to) the proposed Subprocessor except with the prior written consent of Arcadia.

## With respect to each Subprocessor, Vendor shall:

### before the Subprocessor first Processes Arcadia Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Arcadia Data required by the Agreement;

### ensure that the arrangement between on the one hand (a) Vendor or (b) the relevant intermediate Subprocessor and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Arcadia Data as those set out in this Addendum; and

### provide to Arcadia for review such copies of Vendor’s agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Arcadia may request from time to time.

## Vendor shall ensure that each Subprocessor performs the obligations under this Addendum as they apply to the Processing of Arcadia Data as if each Subprocessor were party to this Addendum in place of Vendor. Where a Subprocessor fails to fulfil its data protection obligations, Vendor shall remain fully liable to Arcadia for the performance of such Subprocessor’s obligations.

# **Data Subject Rights**

## Taking into account the nature of the Processing, Vendor shall assist Arcadia by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Arcadia’s obligations, as reasonably understood by Arcadia, to respond to requests to exercise Data Subject rights under any Applicable Laws.

## Vendor shall:

### promptly notify Arcadia if Vendor receives a request from a Data Subject under any Applicable Law in respect of Arcadia Data; and

### not respond to that request except on the documented instructions of Arcadia or as required by Applicable Laws to which Vendor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Arcadia of that legal requirement before Vendor responds to the request.

# **Personal Data Breach**

## Vendor shall notify Arcadia without undue delay (but in no more than 24 hours) upon Vendor becoming aware of an actual or reasonably suspected Personal Data Breach affecting Arcadia Data, providing Arcadia with sufficient information to allow Arcadia to meet any reporting or notification obligations. Vendor’s notification shall as a minimum:

### describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

### communicate the name and contact details of Vendor’s data protection officer or other relevant contact from whom more information may be obtained;

### describe the likely consequences of the Personal Data Breach; and

### describe the measures taken or proposed to be taken to address the Personal Data Breach.

## Notifications made pursuant to section 7.1 shall be directed to [INSERT CONTACT INFORMATION].

## Vendor shall cooperate with Arcadia and take such reasonable commercial steps as are directed by Arcadia to assist in the investigation, mitigation, and remediation of any Personal Data Breach.

## In the event of a Personal Data Breach, Vendor is not authorized to notify a data protection or other authority, the Data Subjects concerned, or any other third parties unless Vendor is required to do so under Applicable Laws. In such event, Vendor shall, to the extent permitted under Applicable Laws, liaise and coordinate with Arcadia prior to making a notification. The parties shall use their best efforts to agree on a joint approach with a view to prevent any contradicting or inconclusive notifications. This includes providing each other with the details of any notification and the date and time on which notification will be made.

# **Data Protection Impact Assessment and Prior Consultation**

## Vendor shall provide reasonable assistance to Arcadia with any data protection impact assessments and prior consultations with data privacy authorities which Arcadia reasonably considers to be required of Arcadia by any Applicable Laws, in each case solely in relation to Processing of Arcadia Data by, and taking into account the nature of the Processing and information available to, Vendor.

## Vendor shall without undue delay (but in no more than 24 hours), and to the extent it is permitted to do so by Applicable Laws, inform Arcadia about (i) any audits, inquiries, orders, administrative or criminal charges, and any other measures or proceedings (including involving Subprocessors) taken by data protection authorities or other public authorities; (ii) any complaints, claims, or civil proceedings initiated by third parties, and (iii) any subpoenas, search warrants, or discovery requests, to the extent that these relate to Arcadia Data or Vendor’s obligations under this Addendum.

# **Deletion or Return of Arcadia Data**

## Subject to sections 9.2 and 9.3, Vendor shall promptly and in any event no later than thirty (30) days after the date of cessation of any Services involving the Processing of Arcadia Data (the “**Cessation Date**”), delete and procure the deletion of all copies of those Arcadia Data in the possession of Vendor and/or any Subprocessor. As used in this section 9, “**delete**” means to remove or obliterate Arcadia Data such that it cannot be recovered or reconstructed.

## Subject to section 9.3, Arcadia may in its absolute discretion by written notice to Vendor no later than thirty (30) days prior to the Cessation Date require Vendor to return a complete copy of all Arcadia Data to Arcadia by secure file transfer in such format as is reasonably notified by Arcadia to Vendor; and (b) delete and procure the deletion of all other copies of Arcadia Data in the possession of Vendor and/or any Subprocessor. Vendor shall comply with any such written request no later than thirty (30) days after the Cessation Date.

## Vendor may retain Arcadia Data only to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor shall ensure the confidentiality of all such Arcadia Data and shall ensure that such Arcadia Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its retention and for no other purpose.

## Vendor shall provide written certification to Arcadia that it has fully complied with this section 9 within sixty (60) days of the Cessation Date.

# **Audit Rights**

## Vendor shall make available to Arcadia on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Arcadia or an auditor mandated by Arcadia in relation to the Processing of the Arcadia Data by Vendor. Vendor shall immediately inform Arcadia if, in its opinion, an instruction pursuant to this section 10 infringes any Applicable Laws.

## Each party shall bear its own costs with respect to any audit unless (i) the audit is performed because Vendor has given Arcadia the notice required by section 2.4 or (ii) it is determined that Vendor has breached this Addendum, in which case Vendor shall reimburse Arcadia for all necessarily incurred costs resulting from the audit.

# **Transfer Mechanisms for United Kingdom and European Data Restricted Transfers**

## **European Union and European Economic Area.** Vendor agrees that it shall abide by the relevant terms of the Standard Contractual Clauses incorporated as Appendix A to this Addendum for Restricted Transfers outside of the European Union and European Economic Area (“**EU SCCs**”). For transfers from Arcadia to Vendor, the EU SCCs shall apply to Arcadia in its role as the “data exporter” and to Vendor in its role as “data importer.” Vendor agrees that, as provided in the EU SCCs, Data Subjects shall be third party beneficiaries to the EU SCCs. In addition, Arcadia and Vendor hereby agree that the security provisions in the Agreement shall apply to EU Annex II of the EU SCCs.

## **United Kingdom.** Vendor agrees that it shall abide by the relevant terms of the Standard Contractual Clauses incorporated as Appendix B to this Addendum for Restricted Transfers outside of the United Kingdom (“**UK SCCs**”). For transfers from Arcadia to Vendor, the UK SCCs shall apply to Arcadia in its role as the “data exporter” and to Vendor in its role as “data importer.” Vendor agrees that, as provided in the UK SCCs, Data Subjects shall be third party beneficiaries to the UK SCCs.

## Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor, Vendor’s entry into the EU SCCs and UK SCCs under section 11.1, and agreement to variations to those SCCs made under section 13.5.1, as agent for and on behalf of that Subprocessor, will have been duly and effectively authorized (or subsequently ratified) by that Subprocessor.

# **LIABILITY AND INDEMNIFICATION**

## Notwithstanding any contrary provisions of the Agreement, Vendor shall be fully liable, without limitation, in accordance with Applicable Laws for any: (i) breach of its duties under this Addendum; (ii) breach of any Subprocessor’s duties; and (iii) any Personal Data Breach, and shall fully indemnify Arcadia and its TRUSTEES, officers, employees, and agents against and hold them harmless from any losses, liabilities, claims, damages, fines, penalties and any other costs (including reasonable costs of investigation and defense and reasonable legal and other professionals’ fees) suffered or incurred based upon, attributable to or arising from any such incidents. To the extent this Addendum is inconsistent with the terms of any contracts comprising the Agreement, this Addendum shall govern.

## Notwithstanding any contrary provisions of the Agreement or this Addendum, Vendor shall indemnify and reimburse Arcadia FOR any and all damages, losses, fees, or costs (whether direct, indirect, special, or consequential) incurred as a result of any (i) breach of its duties under this Addendum; (ii) breach of any Subprocessor’s duties; and (iii) any Personal Data Breach, and remedy any harm or potential harm caused by such incident. Vendor shall fully cooperate with Arcadia AND take such reasonable commercial steps as are directed by Arcadia TO assist in the investigation of any Personal Data Breach or other security incident.

## Arcadia shall not be liable for any additional charges under this Addendum and the parties acknowledge and agree that all costs, charges and fees in connection with this Addendum are fully and adequately compensated by the fees and charges payable under the Agreement.

# **General Terms**

## *Notifications*

## Any notifications made to Arcadia pursuant to this Addendum shall be directed to [INSERT CONTACT INFORMATION].

## *Governing law and jurisdiction*

## Without prejudice to clauses 17 (Governing Law) and 18 (choice of forum and jurisdiction) of the EU SCCs, and clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the UK SCCs:

### the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

### this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

## *Order of precedence*

## Nothing in this Addendum reduces Vendor’s obligations under the Agreement in relation to the protection of Arcadia Data or permits Vendor to Process (or permit the Processing of) Arcadia Data in a manner which is prohibited by the Agreement.

## In the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail. Notwithstanding the foregoing, in the event of any conflict or inconsistency between this Addendum and the applicable set of Standard Contractual Clauses (EU SCCs or UK SCCs), the applicable set of Standard Contractual Clauses shall prevail.

## *Changes in Applicable Laws*

## Arcadia may:

### by at least thirty (30) days’ written notice to Vendor from time to time make any variations to the EU SCCs or UK SCCs (including any standard contractual clauses entered into under section 11.1), as they apply to Restricted Transfers which are subject to a particular Applicable Law, which are required, as a result of any change in, or decision of a competent authority under, that Applicable Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Applicable Law; and

### propose any other variations to this Addendum which Arcadia reasonably considers to be necessary to address the requirements of any Applicable Law.

## If Arcadia gives notice under section 13.5.1, Vendor shall promptly cooperate (and ensure that any affected Subprocessors promptly cooperate) to ensure that equivalent variations are made to any agreement put in place under section 5.

## If Arcadia gives notice under section 13.5.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Arcadia’s notice as soon as is reasonably practicable.

## Neither Arcadia nor Vendor shall require the consent or approval of any Vendor Affiliate to amend this Addendum pursuant to this section 13 or otherwise.

## *Breach*

## In the event of a material breach of Vendor’s duties and obligations under this Addendum which affects the confidentiality, integrity, or security of Arcadia Data, Arcadia shall be entitled to terminate this Addendum and the Agreement for cause with immediate effect. If Arcadia terminates this Addendum and the Agreement pursuant to this Section 13.9, (i) all obligations of Vendor and all rights that Arcadia has under this Addendum shall survive termination and remain in full force and effect, and (ii) any fees/charges paid in advance by Arcadia will be pro-rated and promptly refunded by Vendor.

## *Severance*

## Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement.

**On behalf of Arcadia**

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**On behalf of [VENDOR]**

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### **ATTACHMENT 1: DETAILS OF PROCESSING OF ARCADIA DATA**

### This Attachment 1 includes certain details of the Processing of Arcadia Data and amends the Standard Contractual Clauses incorporated in this DPA as Annex and Annex B, as applicable.

### *The Parties:*

### Data Exporter:

### Name:

### Address:

### Contact person’s name, position and contact details:

### Activities relevant to the data transferred under these Clauses:

### Signature and date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Role: Controller

###  Data Importer:

### Name:

### Address:

### Contact person’s name, position and contact details:

### Activities relevant to the data transferred under these Clauses:

### Signature and date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Role: Processor

### *Categories of data subjects whose personal data is transferred:*

### [Insert].

### *Categories of Personal Data Transferred:*

### [Insert].

### *The types of Arcadia* *Data to be Processed*

[Insert].

### *Sensitive Data Transferred:*

[Insert].

### *The frequency of the transfer:*

### [Insert].

### *Nature of the Processing:*

### [Insert].

### *The period for which the personal data will be retained, or if that is not possible, the criteria used to determine the period:*

### [Insert].

### *Competent Supervisory Authority:*

### [Insert].

### *List of Sub-Processors:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub-processor Name** | **Address** | **Contact person’s name, position and contact details** | **Description of processing** |
|  |  |  |  |
|  |  |  |  |

### **ATTACHMENT 2: Technical and Organizational Measures including Technical and Organizational Measures to endure the Security of the Data**

### [Vendor to complete.]