Data Transfer Addendum (Controller to Controller)

This Data Transfer Addendum (**"Addendum"**) is effective on the first date that Customer provides Personal Data (as defined below) subject to the applicable Privacy Law (as defined below) and forms part of the Master Agreement or other written or electronic agreement (**"Agreement"**) by and between the organization signing or accepting below (**"Customer"**) and **Environmental Systems Research Institute, Inc.** (**"Esri"**), and sets forth the terms and conditions relating to the privacy and security of Customer Personal Data received by Esri as a controller pursuant to the Agreement. All terms defined or used in the Agreement shall have the same meaning in this Addendum unless otherwise specified. Terms used in this Addendum that are not defined herein or in the Agreement shall have the meaning set forth in the applicable Privacy Law. This Addendum applies if Personal Data is subject to the GDPR.

If applicable, each party's signature to this Addendum shall be considered a signature to Attachment 1 Standard Contractual Clauses Implementation (including the annexes).

Whereas Customer may provide Esri, a company located in the United States, with access to Personal Data;

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Esri agree as follows:

SECTION I—DEFINITIONS

A. **"Privacy Laws"** means the European Union (EU) General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"), the California Consumer Protection Act of 2018 (as amended by the California Privacy Rights Act [CPRA]), and other applicable privacy laws.
B. The terms "personal data," "data subject," "processing," "controller," "processor," and "supervisory authority" as used in this Addendum have the meanings given in the GDPR.
C. **"Personal Data"** means personal data provided by Customer to Esri.

SECTION II—PRIVACY AND INFORMATION SECURITY

A. Parties as Controllers

   i. Customer and Esri agree that Esri is a controller of certain Personal Data that is subject to Esri's Privacy Statement found at https://www.esri.com/en-us/privacy/overview.
   ii These Addendum terms do not apply where Esri is a processor of Personal Data received and processed by Esri in accordance with its data processing addendum found at https://www.esri.com/en-us/privacy/privacy-gdpr.

B. Protection of Personal Data

   i. The parties will provide at least the same level of privacy protection for Personal Data as is required by Privacy Laws.
   ii. The parties will reasonably cooperate with each other to address any valid data subject requests.
   iii. 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 of the rights and freedoms of natural persons, the parties will implement appropriate technical and organizational measures to protect the Personal Data from loss; misuse; and unauthorized access, disclosure, alteration, and destruction.
   iv. Esri shall make available to Customer the information necessary to demonstrate compliance with the GDPR. At Customer's request to verify compliance, Esri will provide to Customer a summary of its most recent independent third-party audit results. The summary will be provided no more than once annually, and disclosure of the summary will be subject to a written nondisclosure agreement between the parties. An on-site audit may be conducted by Customer or an independent third-party auditor as agreed by the parties when: (i) such an audit is required by Privacy Law or by Customer's competent supervisory

authority; (ii) the information provided under this section is reasonably insufficient to demonstrate compliance with the obligations set forth in this Addendum; or (iii) Customer has received a notice from Esri of a data incident related to Customer's Personal Data. The scope and scheduling of such audit will be mutually agreed upon by the parties in advance. All expenses resulting from this subsection will be incurred by Customer, unless Esri is found materially noncompliant. Customer must promptly notify Esri of any discovered noncompliance.

v. Esri will not Sell or Share (as defined in the CCPA/CPRA) Personal Data. Esri will not (a) retain, use, or disclose Personal Data outside of the direct business relationship between the parties or for any purpose other than performing under the Agreement, except as otherwise permitted by this Addendum or the Privacy Laws or (b) combine Customer's Personal Data with any other personal information received or collected from or on behalf of another person, provided that Esri may combine personal information for a business purpose (as defined under CCPA/CPRA).

C. Customer certifies that it has:

i. Obtained the written consent, affirmative opt-in, other written authorization (**"Consent"**) from applicable individuals or has another legitimate, legal basis for delivering or making accessible Personal Data to Esri (as well at its subsidiaries, affiliates, and processors) and such Consent or other legitimate basis allows Esri (and its subsidiaries, affiliates, and processors) to receive and process Personal Data pursuant to the terms of the Agreement and this Addendum, and

ii. Ensured that the delivery and disclosure of Personal Data to Esri is in compliance with the GDPR and other Privacy Laws.

ESRI CERTIFIES THAT IT AND ITS EMPLOYEES UNDERSTAND THESE RESTRICTIONS AND WILL COMPLY WITH THEM.

IN WITNESS WHEREOF, the parties acknowledge their agreement to the foregoing by due execution of this Addendum by their respective authorized representatives. This Addendum cannot be modified or amended by either party except with a separate written document signed by both parties.

_____	ENVIRONMENTAL SYSTEMS RESEARCH INSTITUTE, INC.
(Customer)	(Esri)
By: _____	By: _____
Authorized Signature	Authorized Signature
Printed Name: _____	Printed Name: Tamisa Greening
Title: _____	Title: Director of Contracts and Legal
Date: _____	
Customer Number: _____	

ATTACHMENT 1
STANDARD CONTRACTUAL CLAUSES IMPLEMENTATION

1. The parties agree that, with respect to the implementation of the standard contractual clauses under this Addendum, Module One ("Controller to Controller") shall apply.

2. To the extent Module 1 applies, the parties agree to the following:

   (a) Clause 7 (Docking Clause) shall not apply;
   (b) Clause 11(a) (Redress) option shall not apply;
   (c) Governing law under Clause 17 (Governing law) shall be law of the Republic of Ireland; and
   (d) Clause 18 (Choice of forum and jurisdiction) shall mean the courts of the Republic of Ireland.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Name:** As identified in the Agreement and this Addendum

   Address: Per Esri's customer service records

   Contact person's name, position, and contact details: Per Esri's customer service records

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

   Signature and date: Each party's signature on this Addendum shall be considered a signature to these Clauses.

   Role (controller/processor): Controller

Data importer(s):

1. **Name:** Environmental Systems Research Institute, Inc. ("Esri")

   Address: 380 New York Street, Redlands, CA 92373 USA

   Contact person's name, position, and contact details: Chief Information Security Officer, privacy@esri.com

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

   Signature and date: Each party's signature on this Addendum shall be considered a signature to these Clauses.

   Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer employees and other data subjects whose personal data is provided by Customer to Esri for the purpose of performance of the Agreement or otherwise subject to Esri's Privacy Statement found at https://www.esri.com/en-us/privacy/overview

Categories of personal data transferred

Categories of personal data that are subject to Esri's Privacy Statement found at https://www.esri.com/en-us/privacy/overview

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A.

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

It is expected that transfers may be one-off and/or continuous.

Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing

As necessary for performance of the Agreement and as otherwise described in Esri's Privacy Statement found at https://www.esri.com/en-us/privacy/overview.

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

As necessary for performance of the Agreement, compliance with laws and for legitimate interests of the controller.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

As described in Esri's Privacy Statement found at https://www.esri.com/en-us/privacy/overview

C. COMPETENT SUPERVISORY AUTHORITY

As applicable in accordance with Clause 13.

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

Description of the technical and organisational security measures implemented by the data importer in accordance with GDPR:

A. TECHNICAL MEASURES

Esri may employ any of the following technical and organisational controls to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

i. Penetration testing to ensure the security of systems.
ii. Encrypting data in transit over public resources using at least TLS 1.2, using certificates from recognized Certificate Authorities to ensure the authenticity of connections can be validated.
iii. Encrypting laptop devices using centralized software to enforce the configuration of the encryption using recognized public algorithms and ensuring central management of the encryption key.
iv. Maintaining an Incident Response Plan that is reviewed annually to be executed by our internal Security Operations Center in the event of a suspected breach.
v. Restricting physical access using layers of physical controls such as key card locks, cipher locks, and video cameras. Esri also relies on third-party data centers to provide physical protection for data.
vi. Collecting and analyzing event logs from computing devices, network devices, and key applications via a central SIEM for anomalies and indicators of compromise.
vii. Installing patches and end-point protection programs such as antivirus and EDR using remote management software.
viii. Protecting access to privileged credentials and restricting remote access using multifactor authentication.
ix. Redistricting access to sensitive systems by segmenting networks and using identity-based firewall rules to restrict access to sensitive systems.
x. Detecting anomalous behaviors on networks using IDS/IPS devices.
xi. Implementing principals of least privilege that grant a limited set of access to employees by default and ensuring that additional access must be requested and approved by the system owner or their designated representatives.
xii. Ensuring availability by performing regular backups of datasets identified as requiring restoration in the event of a data loss event and applying encryption to those backups when it is identified as necessary.
xiii. Reviewing and managing risk associated with third parties.

B. ORGANIZATIONAL AND CONTRACTUAL MEASURES

i. Esri's efforts around privacy are described at https://www.esri.com/en-us/privacy/overview.
ii. Esri commits to treating Personal Data per its Privacy Statement (available here: https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement) and Esri Products & Services Privacy Statement Supplement (available here: https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement).
iii. Esri maintains and enforces an internal Personal Information Protection Policy that requires employees to protect Personal Data that they access.
iv. Esri maintains a Corporate Security Policy that addresses access controls and corporate security measures.

Customer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data in accordance with applicable Privacy Laws.