

This Data Processing Addendum ("**Addendum**") is effective on the first date that Customer provides to Esri EU Personal Data (as defined below) subject to the GDPR (as defined below) or May 25, 2018, whichever is later, 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, confidentiality, and security of EU Personal Data associated with Online Services and Maintenance to be rendered by Esri to Customer pursuant to the Agreement. All terms defined or used in the Agreement shall have the same meaning in this Addendum unless otherwise specified.

Whereas Customer may provide Esri, a company located in the United States, with access to personally identifiable information about individuals located in the European Union to act as a Processor in connection with Online Services and Maintenance performed by Esri for or on behalf of Customer pursuant to the Agreement; and

Whereas Customer requires that Esri preserve and maintain the privacy and security of such EU Personal Data as a Processor according to the terms of this Addendum;

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. "**GDPR**" means the European Union General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- B. "**Privacy Shield**" means the EU-US Privacy Shield framework and Swiss-US Privacy Shield framework.
- C. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this Addendum have the meanings given in the GDPR.
- D. "**EU Personal Data**" means personal data about individuals located in the European Union, Switzerland or the United Kingdom and may include, but not limited to, the following: (i) categories of data subjects: prospects, customers, business partners, and vendors and (ii) types of personal data: name, title, position, and email address and location.
- E. "**Data Incident**" means a breach of Esri's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, EU Personal Data on systems managed by or otherwise controlled by Esri. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of EU Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

SECTION II—PRIVACY, CONFIDENTIALITY, AND INFORMATION SECURITY

- A. Authority to Process EU Personal Data
 - i. Customer and Esri agree that Customer is the Controller and Esri is the Processor of EU Personal Data, except when Customer is a Processor of EU Personal Data, then Esri is a subprocessor.
 - ii. These Addendum terms do not apply where Esri is a Controller of EU Personal Data (e.g., EU Personal Data received and Processed by Esri as needed for account setup, authorization, and sign on).
 - iii. Esri will Process EU Personal Data only with Customer's written instructions, (a) on behalf of and for the benefit of Customer; (b) for the purposes of Processing EU Personal Data in connection with the Agreement; and (c) to carry out its obligations pursuant to this Addendum, the Agreement, and by law.
 - iv. Customer will have the exclusive authority to determine the purposes for and means of Processing EU Personal Data.
 - v. The subject matter and details of the processing are described on Appendix 1 and this Addendum including the Appendix and the Agreement are Customer's complete instructions to Esri for the

Processing of EU Personal Data. Any alternative or additional instructions may only be by written amendment to this Addendum.

B. Disclosure of and Access to EU Personal Data

- i. Esri will hold in confidence all EU Personal Data.
- ii. Esri will (a) provide at least the same level of privacy protection for EU Personal Data received from Customer, as is required by the GDPR, and the Privacy Shield principles that may be found on the Privacy Shield [website](#); (b) promptly notify Customer if at any time Esri determines that it can no longer meet its obligation to provide the same level of protection as is required by the GDPR; and (c) take reasonable and appropriate steps to remediate the Processing of such EU Personal Data if, at any time, Customer notifies Esri that Customer has reasonably determined Esri is not Processing the EU Personal Data in compliance with the GDPR.
- iii. Esri will only transfer EU Personal Data outside the country in which Customer or its personnel originally delivered it to Esri for Processing (or, if it was originally delivered to a location inside the European Economic Area [EEA] or Switzerland), outside the EEA or Switzerland where adequate data privacy safeguards are in place, such as binding corporate rules, the Model Clauses, or the Privacy Shield principles, unless required by law, in which case, Esri will, unless such prior disclosure is prohibited, notify Customer of such requirement before Processing.
- iv. Esri will not share, transfer, disclose, or otherwise provide access to any EU Personal Data to any third party or contract any of Esri's rights or obligations concerning EU Personal Data to a third party, unless Customer has authorized Esri to do so in writing, except as required by law. Where Esri, with the consent of Customer, provides to a third party access to EU Personal Data or contracts such rights or obligations to a third party, Esri will, with each third party, (a) enter into a written agreement that imposes obligations on the third-party that are consistent with the GDPR, (b) transfer the EU Personal Data to the third party only for the limited and specified purposes as instructed by Customer, (c) require the third party to notify Esri if the third party determines that it can no longer meet its obligation to provide the same level of protection as is required by the GDPR; and (d) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing. Customer hereby provides its consent for Esri to use subprocessors as necessary to provide the services including, but not limited to, use Microsoft Corporation, Amazon Web Services, Inc., and Salesforce.com, Inc. and their affiliates. To the extent that Esri makes any changes with regard to the use of its subprocessors, it shall inform Customer and provide Customer with the right to object to such change. To the extent Customer has a reasonable objection to such change in subprocessors, the parties shall cooperate to address the objection in a reasonable manner.
- v. Esri will promptly inform Customer in writing of any requests with respect to EU Personal Data received from Customer's customers, consumers, employees, or other associates. Customer will be responsible for responding to any such request, but Esri will reasonably cooperate with Customer to address any such request or a request by an individual about whom Esri holds EU Personal Data for access, rectification, objection, portability, restriction, erasure, or export of his or her EU Personal Data.
- vi. 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, Esri will implement appropriate technical and organizational measures to protect the EU Personal Data from loss; misuse; and unauthorized access, disclosure, alteration, and destruction. To this effect, Esri will limit internal access to EU Personal Data so that it is only accessible on a need-to-know basis to fulfill Esri's performance of services for or on behalf of Customer, by employees who have agreed to comply with privacy and security obligations that are substantially similar to those required by this Addendum.
- vii. Subject to applicable law, Esri will notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of EU Personal Data. Customer may, if it so chooses, seek a protective order, and Esri will reasonably cooperate with Customer in such action, provided Customer reimburses Esri for all costs, fees, and legal expenses associated with the action. Esri will have the right to approve or reject any settlements that affect Esri.
- viii. If Esri becomes aware of a Data Incident, Esri will: (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to

minimize harm and secure EU Personal Data. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Esri recommends Customer take to address the Data Incident. Esri will not assess the contents of EU Personal Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any notification obligations to third parties related to any Data Incident(s). Esri's notification of or response to a Data Incident under this section will not be construed as an acknowledgement by Esri of any fault or liability with respect to the Data Incident.

- C. Esri currently has the third-party certifications and review processes in place as described at <http://trust.arcgis.com>.
- D. Esri will comply with applicable data protection and privacy laws, including, but not limited to, the GDPR, to the extent such laws apply to Esri in its role as a Processor.
- E. Customer certifies that it has:
 - i. Obtained the written consent, affirmative opt-in, other written authorization ("**Consent**") from applicable individuals in the European Union or has another legitimate, legal basis for delivering or making accessible EU Personal Data to Esri (as well as its subsidiaries, affiliates, and subprocessors), and such Consent or other legitimate basis allows Esri (and its subsidiaries, affiliates, and subprocessors) to Process the EU Personal Data pursuant to the terms of the Agreement and this Addendum, and
 - ii. Ensured that the delivery and disclosure to Esri of EU Personal Data is in compliance with the GDPR as Controller and all laws applicable to Customer and otherwise complies with applicable privacy and data protection laws.
- F. Esri will assist Customer in ensuring that its secure Processing obligations, as Controller, under the GDPR are met, which may include assisting Customer in a consultation with a supervisory authority where a data protection impact assessment indicates that the intended Processing would result in a high risk. Upon request, Esri shall make available to Customer the information necessary to demonstrate compliance with the GDPR and will allow for and contribute to audits, including inspections, to confirm Esri's compliance with this Addendum by Controller or another auditor mandated by Controller. All expenses resulting from this Subsection F will be incurred by Customer, unless Esri is found materially noncompliant.
- G. Upon termination of the Agreement, Esri shall either return all EU Personal Data Processed on behalf of Customer or delete or destroy the EU Personal Data, including any existing copies, at Customer's expense, if any, unless Esri has a legal obligation to maintain such EU Personal Data.

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

(Customer)

By: _____
Authorized Signature


Printed Name: _____

Title: _____

Date: _____

Customer Number: _____

ENVIRONMENTAL SYSTEMS
RESEARCH INSTITUTE, INC.
(Esri)

By:  _____
Authorized Signature

Printed Name: William C. Fleming

Title: Director, Contracts and Legal

Date: _____

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Esri's provision of the Online Services and Maintenance to Customer.

Duration of the Processing

The Term plus the period from the expiry of the Term until deletion of all EU Personal Data by Esri in accordance with the Agreement.

Nature and Purpose of the Processing

Esri will process EU Personal Data for the purposes of providing the Online Services and Maintenance to Customer in accordance with the Agreement.

Categories of Data

Data relating to individuals provided to Esri via the Online Services and Maintenance, by (or at the direction of) Customer or by Customer End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Esri via the Online Services and Maintenance by (or at the direction of) Customer or by Customer End Users.

Technical and Organizational Measures for Security

Details of technical and organizational security measures are described here:
<https://doc.arcgis.com/en/trust/security/security-overview.htm>