Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is effective on the first date that Customer provides to Esri 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, confidentiality, and security of Personal Data associated with Online Services and subscription and maintenance services 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. Terms used in this Addendum which are not defined herein or in the Agreement shall have the meaning set forth in the applicable Privacy Law.

Whereas Customer may provide Esri, a company located in the United States, with access to Personal Data, Personal Information or Personally Identifiable Information to act as a Processor or Service Provider in connection with Online Services and subscription and maintenance services 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 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. "**Privacy Laws**" means the European Union General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, The California Consumer Privacy Act of 2018 or other privacy laws applicable to Esri.
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, Personal Information or Personally Identifiable Information as defined in applicable Privacy Laws about individuals located in the European Union, Switzerland, the United Kingdom, California or other locations covered by Privacy Laws 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.
D. **"Data Incident"** means a breach of Esri's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, 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 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 Personal Data

   i. Customer and Esri agree that Customer is the Controller and Esri is the Processor or Service Provider of Personal Data, except when Customer is a Processor of Personal Data, then Esri is a subprocessor.
   ii These Addendum terms do not apply where Esri is a Controller of Personal Data (e.g., Personal Data received and Processed by Esri as needed for account setup, authorization, and sign on).
   iii. Esri will Process Personal Data only with Customer's written instructions, (a) on behalf of and for the benefit of Customer; (b) for the purposes of Processing Personal Data in connection with the Agreement; and (c) to carry out its obligations pursuant to this Addendum, the Agreement, and applicable Privacy Laws and other law.

iv. Customer will have the exclusive authority to determine the purposes for and means of Processing Personal Data.
v. The subject matter and details of the processing are described in Appendix 1 of Annex 1, and this Addendum, including the Annex, Appendices, and the Agreement, are Customer's complete instructions to Esri for the Processing of Personal Data. Any alternative or additional instructions may only be by written amendment to this Addendum.

B. Disclosure of and Access to Personal Data

i. Esri will hold in confidence all Personal Data. Esri will not Sell Personal Data.
ii. Esri will (a) provide at least the same level of privacy protection for Personal Data received from Customer, as is required by the GDPR, CCPA and other applicable Privacy Laws; (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 Privacy Laws; and (c) take reasonable and appropriate steps to remediate the Processing of such Personal Data if, at any time, Customer notifies Esri that Customer has reasonably determined Esri is not Processing the Personal Data in compliance with the Privacy Laws.
iii. If Esri Processes Personal Data provided by Customer that is subject to the GDPR and Esri is established in, or transfers or makes accessible any Personal Data to any subprocessors in a country that does not ensure adequate data privacy safeguards are in place within the meaning of GDPR, then Esri will enter into the standard contractual clauses with Customer as set forth in Annex 1 of this Addendum. If applicable, each party's signature to this Data Processing Addendum shall be considered a signature to the standard contractual clauses (including the appendices). If a subprocessor is a Data Importer (as that term is used in such standard contractual clauses under GDPR), Esri shall either (a) enter into contractual obligations with subprocessor, where such obligations contain adequate privacy safeguards in accordance with GDPR or (b) enter into the standard contractual clauses with Customer on behalf of such data importer.
iv. Esri will not share, transfer, disclose, or otherwise provide access to any Personal Data to any third party, or contract any of Esri's rights or obligations concerning 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 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, CCPA and the other Privacy Laws, (b) transfer the 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 applicable Privacy Laws; 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 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 Personal Data for access, rectification, objection, portability, restriction, erasure, or export of his or her 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 Personal Data from loss; misuse; and unauthorized access, disclosure, alteration, and destruction. To this effect, Esri will limit internal access to 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 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 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 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 https://trust.arcgis.com.

D. Esri will comply with applicable data protection and privacy laws, including, but not limited to, the GDPR and CCPA, to the extent such laws apply to Esri in its role as a Processor or Service Provider.

E. 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 subprocessors), and such Consent or other legitimate basis allows Esri (and its subsidiaries, affiliates, and subprocessors) to Process the Personal Data pursuant to the terms of the Agreement and this Addendum, and

ii. Ensured that the delivery and disclosure to Esri of Personal Data is in compliance with the GDPR, CCPA and other Privacy Laws which are applicable to Customer.

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 fulfillment of the purpose for which Customer provided Personal Data under this Addendum, Esri shall either return all Personal Data Processed on behalf of Customer or delete or destroy the Personal Data, including any existing copies, at Customer's expense, if any, unless Esri has a legal obligation to maintain such 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.

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

ANNEX 1
Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel.: .....; fax: .....; e-mail: .....

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Environmental Systems Research Institute, Inc. (the data importer), an entity incorporated in the State of California with principal offices located at 380 New York Street, Redlands, California 92373-8100

Tel. 909-793-2853

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in **Appendix 1** which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in **Appendix 2** before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

If we get a subpoena to disclose from the authorities we need to tell whoever gave us the PII

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …….

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ……
……

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): .....

Signature …….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): .....

Signature …….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Subject Matter and Details of the Data Processing

This Appendix forms part of the Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Subject Matter

Esri's provision of the Online Services and subscription and maintenance services to Customer.

Duration of the Processing

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

Nature and Purpose of the Processing

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

Categories of Data

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

Subprocessor Agreement Scope

In accordance with Esri's obligation to make available to the data subject, upon request, a copy of any existing contract Esri has with its subprocessors, Esri will only make availble portions or summaries of such contracts to the extent necessary (in Esri's reasonable discretion) for the data subject to ensure adequate protection of his or her Personal Data.

Audit Scope

At Customer’s request to verify compliance with Esri’s obligations under this Addendum, Esri will provide to Customer a summary of its most recent independent third party FedRAMP 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.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Technical and Organisational Security Measures

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

Esri will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to ArcGIS Online Services and subscription and maintenance services, as described in the Security and Privacy Documentation applicable to the specific ArcGIS Online Services and subscription and maintenance services purchased by the data exporter, as updated from time to time, and accessible via https://trust.arcgis.com/en/security/security-overview.htm or otherwise made reasonably available by Esri.

A. Government Requests for Customer Personal Data

i. If Esri receives a valid and binding order ("Request") from any governmental body ("Requesting Party") for disclosure of Customer Personal Data, Esri will use reasonable efforts to redirect the Requesting Party to request Customer Personal Data directly from Customer.
ii. If obligated to disclose Customer Personal Data to a Requesting Party, Esri will:

   a. Promptly notify the Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if Esri is legally permitted to do so; or,
   b. If Esri is prohibited from notifying Customer about the Request, use reasonable efforts to obtain a waiver of prohibition to allow Esri to communicate to Customer as much information as it can as soon as possible and challenge an overbroad Request or a Request that does not meet legal requirements.

iii. If, after exhausting the steps described in Section 2 above, Esri remains obligated to disclose Customer Personal Data to a Requesting Party, Esri will disclose only the minimum amount of Customer Data necessary to satisfy the Request.

B. Technical Measures for ArcGIS Online Services. Esri implemented the following technical measures for the above referenced ArcGIS Online Services:

i. The state-of-the-art encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) are used for Customer data at rest.
ii. The strength of the encryption takes into account the time period during which the confidentiality of the encrypted personal data must be preserved.
iii. The encryption algorithm is implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified by certification.
iv. The keys are reliably managed (generated, administered, stored, linked to the identity of an intended recipient, and revoked).
v. ArcGIS Online allows the Customer (data exporter) to pseudonymize the fields (e.g., user credentials) in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information exclusively held and controlled by Customer (data exporter), of which the Customer (data exporter) retains sole control of the algorithm or repository that enables reidentification using additional information.
vi. ArcGIS Online supports best practices for transport encryption protocols.
vii. A trustworthy public key certification authority and infrastructure are used.
viii. Specific protective and state-of-the-art measures are used against active and passive attacks.
ix. The existence of backdoors (in hardware or software) has been ruled out.

x. ArcGIS Online can be used in combination with ArcGIS Enterprise in a configuration that allows the Customer (data exporter) to store and manage Personal Data under Customer's (data exporter's) control without transferring it to a third country, whereas a data exporter processes Personal Data in such a manner that it is split into two or more parts, and the part that is being transferred to the third country can no longer be interpreted or attributed to a specific data subject without the use of additional information under the Customer's (data exporter's) control.

Additional information on technical measures can be found here: https://trust.arcgis.com/en/documents/

C. 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/enus/privacy/privacy-statements/privacy-supplement).
iii. Esri provides a presigned Data Processing Addendum that contains Standard Contractual Clauses here: https://www.esri.com/en-us/privacy/privacy-gdpr.
iv. Esri maintains and enforces an internal Personal Information Protection Policy that requires employees to protect Personal Data that they access.
v. Esri maintains a Corporate Security Policy that addresses access controls and corporate security measures.

D. Adoption of Further Requirements and Right to Early Termination. If supervisory authorities adopt further requirements and measures with regard to the transfer of Personal Data to the US (e.g., the adoption of new Standard Contractual Clauses), Esri will amend this Addendum to fulfill the additional requirements. If Esri cannot meet the additional requirements, Customer shall have the right to terminate the Agreement for convenience (without termination fee or penalty) by giving written notice thereof to Esri.