

Le présent Addenda relatif au traitement des Données à caractère personnel (« **Addenda** ») prend effet à la première date à laquelle le Client fournit à Esri des Données à caractère personnel (comme définies ci-dessous) soumises à la Législation relative au respect de la vie privée en vigueur comme définie ci-dessous et fait partie du Contrat ou de tout autre contrat écrit ou électronique (« **Contrat** ») conclu entre le client ci-après (« **Client** ») et **Environmental Systems Research Institute, Inc.** (« **Esri** »), et énonce les conditions générales relatives à la vie privée, à la confidentialité et à la sécurité des Données à caractère personnel associées aux Online Services et aux services d'abonnement et de maintenance fournis par Esri au Client conformément au Contrat. Toutes les dispositions définies ou utilisées dans le Contrat ont la même signification dans cet Addenda, sauf indication contraire. Les termes utilisés dans cet Addenda qui ne sont pas définis dans les présentes ou dans le Contrat auront la signification qui leur est attribuée dans la Législation relative au respect de la vie privée applicable.

Considérant que le Client est autorisé à fournir à Esri, société établie aux États-Unis, un accès aux Données à caractère personnel, afin d'agir en qualité de Sous-traitant ou de prestataire de services dans le cadre des Online Services et des services d'abonnement et de maintenance qui seront fournis par Esri pour ou au nom du Client conformément au Contrat ; et

Considérant que le Client exige qu'Esri préserve et maintienne le caractère privé et la sécurité de telles Données à caractère personnel en tant que Sous-traitant conformément aux dispositions du présent Addenda ;

En conséquence, compte tenu des engagements et accords mutuels décrits dans le présent Addenda et le Contrat et pour toute autre contrepartie adéquate et valable, dont la réception et le caractère suffisant sont attestés par la présente, le Client et Esri conviennent de ce qui suit :

SECTION I—DÉFINITIONS

- A. « **Législation relative au respect de la vie privée** » désigne le Règlement général sur la protection des données (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), le « California Consumer Privacy Act » (CCPA - Loi sur la protection du consommateur de Californie) de 2018 (tel que modifié par le California Privacy Rights Act (CPRA - Loi sur la protection de la vie privée de Californie) ou toute autre législation relative au respect de la vie privée applicable à Esri.
- B. Les termes « données à caractère personnel », « personne concernée », « traitement », « responsable du traitement », « sous-traitant » et « autorité de contrôle » utilisés dans le présent Addenda auront le sens qui leur est donné dans le RGPD.
- C. « **Données à caractère personnel** » désigne les données à caractère personnel, des informations personnelles ou des informations d'identification personnelle, telles que définies dans la Législation relative au respect de la vie privée, se rapportant à des citoyens de l'Union européenne, de Suisse, du Royaume-Uni, de Californie - États-Unis, ou de tout autre lieu couvert par celle-ci et peut inclure, sans toutefois s'y limiter, ce qui suit : (i) catégories de personnes concernées : clients potentiels, clients, partenaires commerciaux et fournisseurs et (ii) types de données à caractère personnel : nom, titre, poste, adresse électronique et position géographique.
- D. « **Incident touchant des données** » désigne une atteinte à la sécurité d'Esri entraînant la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite sur des systèmes gérés ou autrement contrôlés par Esri. Les Incidents touchant des données ne comprennent pas les tentatives infructueuses ou les activités qui ne compromettent pas la sécurité des Données à caractère personnel, y compris les tentatives d'authentification, les requêtes pings, les analyses de ports, les attaques par déni de services et les autres attaques réseau sur des pare-feu ou systèmes en réseau qui sont infructueuses.
- E. « **Data Privacy Framework** » ou « Cadre de protection des données » désigne le cadre de protection des données UE-États-Unis (DPF EU-USA), l'extension britannique du DPF EU-USA et le cadre de protection des données Suisse-États-Unis (DPF Suisse-USA).

SECTION II—VIE PRIVÉE, CONFIDENTIALITÉ ET INFORMATIONS SUR LA SÉCURITÉ

A. Autorité pour traiter des Données à caractère personnel

- i. Le Client et Esri conviennent que le Client est le Responsable du traitement et Esri le Sous-traitant des Données à caractère personnel ou le prestataire de services à ce titre, sauf lorsque le Client est un Sous-traitant de Données à caractère personnel, auquel cas Esri est sous-traitant ultérieur.
- ii. Les dispositions du présent Addenda ne s'appliquent pas lorsqu'Esri est Responsable du traitement des Données à caractère personnel (par exemple, Données à caractère personnel reçues et traitées par Esri selon les besoins pour la configuration, l'autorisation et la connexion au portail en libre-service My Esri). La Déclaration de confidentialité d'Esri (disponible à l'adresse <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>), ainsi que tous avis ou déclarations de confidentialité associés, et le Contrat de transfert de données s'appliquent lorsqu'Esri est Responsable du traitement.
- iii. Esri ne traitera des Données à caractère personnel que sur instructions écrites du Client, (a) au nom ou dans l'intérêt du Client ; (b) à des fins de Traitement de Données à caractère personnel dans le cadre du Contrat ; et (c) pour remplir ses obligations conformément au présent Addenda, au Contrat et à la Législation relative au respect de la vie privée ou toute autre législation.
- iv. Le Client disposera de l'autorité exclusive pour déterminer les finalités et les moyens du traitement des Données à caractère personnel. Esri s'interdira de (a) conserver, utiliser ou divulguer des Données à caractère personnel hors de la relation commerciale directe entre les parties ou à toutes fins autres que l'exécution du Contrat, sauf tel qu'autorisé par le présent Addenda ou les Législations relatives au respect de la vie privée ; ou (b) combiner les Données à caractère personnel du Client avec toute autre information personnelle reçue ou collectée auprès d'une autre personne ou pour le compte de celle-ci, sous réserve qu'Esri puisse combiner des informations personnelles à des fins commerciales (tel que défini en vertu du CCPA/CRPA).
- v. L'objet et les détails du traitement figurent à l'Annexe 1 et le présent Addenda (y compris les Annexes) et le Contrat constituent les instructions complètes du Client dont dispose Esri pour le Traitement des Données à caractère personnel. Toute instruction différente ou supplémentaire ne peut être apportée que par voie d'un avenant écrit au présent Addenda.
- vi. Dans la mesure où le Client divulgue ou met à disposition d'Esri des données anonymisées (tel que défini en vertu du CCPA/CRPA ou toutes autres Législations relatives au respect de la vie privée) ou qu'Esri crée des données anonymisées à partir de Données à caractère personnel, Esri devra (a) prendre des mesures raisonnables pour garantir que les données anonymisées ne soient pas utilisées pour déduire des informations au sujet de toute personne physique ou foyer ou autrement être liées à ces derniers ; (b) s'engager publiquement à conserver et utiliser ces données anonymisées sous forme anonymisées et à ne pas tenter d'identifier les données anonymisées ; et (c) avant de partager des données anonymisées avec tout affilié ou tiers, notamment sous-traitants, sous-traitants ultérieurs ou toutes autres personnes (les « Destinataires »), obliger contractuellement les Destinataires à respecter les exigences de la présente section. Nonobstant la phrase précédente, Esri peut tenter d'identifier les données uniquement aux fins de déterminer si ses processus d'identification de données anonymisées respecte les Législations relatives au respect de la vie privée.

B. Communication et accès aux Données à caractère personnel

- i. Esri préservera la confidentialité de toutes les Données à caractère personnel. Esri ne Vendra ou ne Partagera pas (tel que ces termes sont définis dans le CCPA/CRPA) des Données à caractère personnel.
- ii. Esri (a) fournira au moins le même niveau de protection de la vie privée pour les Données à caractère personnel du Client que celui exigé par le RGPD, le CCPA et toute autre Législation relative au respect de la vie privée, ainsi que les principes du Data Privacy Framework, disponibles sur le [site Internet](#) du Data Privacy Framework ; (b) informera dans les meilleurs délais le Client si, à un moment donné, Esri détermine qu'il n'est plus en mesure de remplir son obligation de fournir le même niveau de protection que celui exigé par la Législation relative au respect de la vie privée et par le Data Privacy Framework, et (c) prendra des mesures raisonnables et appropriées pour remédier au traitement desdites Données à caractère personnel. Si, à tout moment, le Client indique à Esri qu'il estime raisonnablement qu'Esri ne procède pas au Traitement des Données à caractère personnel dans le respect des Législations relatives

au respect de la vie privée, le Client pourra prendre des mesures raisonnables et adéquates pour mettre un terme et remédier à tout Traitement non autorisé desdites Données à caractère personnel.

- iii. Si Esri traite des Données à caractère personnel fournies par le Client qui sont soumises au RGPD et si Esri est établie ou transfère ou permet l'accès à des Données à caractère personnel à tout Sous-traitant ultérieur dans un pays qui n'offre pas de garanties adéquates en matière de respect de la vie privée au sens du RGPD, alors Esri conclura des clauses contractuelles types avec le Client comme cela est évoqué en Annexe 1 du présent Addenda (« CCT ») ou veillera à ce que des mesures de protection des données adéquates soient mises en place, notamment des règles d'entreprise contraignantes ou une certification en vertu du Data Privacy Framework. Le cas échéant, la signature de chaque partie au présent Addenda sera considérée comme une signature des CCT. Si un sous-traitant ultérieur est un Importateur de données (de la manière dont ce terme est utilisé dans lesdites CCT en vertu du RGPD), Esri devra soit (a) conclure des obligations contractuelles avec le sous-traitant ultérieur qui prévoient des garanties en matière de respect de la vie privée conformes au RGPD, soit (b) conclure des CCT avec le client pour le compte de l'Importateur de données en question. Dans l'hypothèse où le transfert est couvert par plusieurs mécanismes, le transfert de données à caractère personnel sera soumis à un seul mécanisme de transfert, le cas échéant, conformément à l'ordre de priorité suivant : (a) le Data Privacy Framework ; (b) les CCT ; et si aucun mécanisme susmentionné ne s'applique, (c) tout autre mécanisme de transfert de donnée alternatif autorisé en vertu des Législations relatives au respect de la vie privée.
- iv. Esri ne partagera, transfèrera et divulguera aucune des Données à caractère personnel à un tiers, n'y donnera pas autrement accès ou ne sous-traitera aucun de ses droits ni aucune de ses obligations concernant les Données à caractère personnel à un tiers, à moins que le Client n'ait autorisé par écrit Esri à le faire, sauf dans les cas prévus par la loi. Lorsqu'Esri, avec l'accord du Client, fournit à un tiers un accès aux Données à caractère personnel ou sous-traite ses droits ou obligations à un tiers, Esri doit, avec chaque tiers, (a) conclure un contrat écrit qui impose au tiers des obligations conformes au RGPD, au CCPA et à toute autre Législation relative au respect de la vie privée ; (b) transférer les Données à caractère personnel au tiers uniquement aux fins spécifiques et limitées établies par le Client, (c) exiger que le tiers informe Esri si le tiers détermine qu'il n'est plus en mesure de remplir son obligation de fournir le même niveau de protection que celui exigé par la Législation relative au respect de la vie privée, et (d) après notification, prendre des mesures raisonnables et appropriées pour stopper le traitement non autorisé et y remédier. Le Client consent par la présente à ce qu'Esri sollicite des sous-traitants ultérieurs si cela est nécessaire pour fournir les services y compris, sans toutefois s'y limiter, Microsoft Corporation, Amazon Web Services, Inc., Salesforce, Inc., et Akamai Technologies (y compris leurs filiales) et les fournisseurs de support technique d'Esri. Dans la mesure où Esri apporte des modifications en rapport avec l'utilisation de ses sous-traitants ultérieurs, il doit en informer le Client et accorder à ce dernier le droit de s'opposer à de telles modifications. Dans la mesure où le Client fait état d'une objection raisonnable au changement de sous-traitants, les parties doivent coopérer pour traiter l'objection d'une manière raisonnable.
- v. Esri informera par écrit le Client dans les meilleurs délais de toutes les demandes concernant les Données à caractère personnel reçues de clients, consommateurs, employés ou d'autres associés du Client. Le Client est tenu de prendre des mesures et de répondre à de telles demandes, mais Esri coopérera raisonnablement avec le Client pour répondre à de telles demandes ou à une demande d'accès, de rectification, d'objection, de portabilité, de restriction, d'effacement ou d'exportation faite par une personne dont Esri détient les Données à caractère personnel. À toutes fins utiles, le Client est un Responsable du traitement des Informations d'identification d'un Utilisateur Nommé, tel que défini dans le Contrat de Licence. Le Client est seul responsable de prendre des mesures et de répondre à toute demande de personne concernée associée aux Informations d'identification d'un Utilisateur Nommé.
- vi. Compte tenu de l'état des connaissances et des coûts de mise en œuvre, et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, Esri doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel de l'UE contre tout(e) perte, utilisation abusive et accès non autorisé, communication, modification et destruction. Lesdites mesures sont décrites en Annexe II des CCT. À cet effet, Esri limitera l'accès interne aux Données à caractère personnel afin qu'elles ne soient accessibles que selon le principe du besoin d'en connaître pour permettre l'exécution des services d'Esri pour ou au nom du Client, par le personnel qui a accepté de se conformer aux obligations de confidentialité et de sécurité substantiellement similaires à celles exigées par le présent Addenda.

- vii. Sous réserve de la législation en vigueur, Esri informera le Client immédiatement par écrit de toute assignation ou autre décision judiciaire ou administrative d'une autorité gouvernementale ou de toute procédure visant à accéder aux Données à caractère personnel ou à les communiquer. Le Client peut, s'il le souhaite, demander une mesure conservatoire, et Esri coopèrera raisonnablement avec le Client dans une telle action, sous réserve que le Client rembourse Esri de la totalité des coûts, dépenses et frais juridiques associés à cette action. Esri pourra approuver ou rejeter les règlements concernant Esri.
- viii. Si un Incident touchant des données est porté à sa connaissance, Esri (a) signalera au Client cet Incident touchant des données immédiatement et sans retard indu après avoir été informé, et (b) prendra immédiatement toutes les mesures raisonnables pour réduire au maximum le risque de préjudice et pour sécuriser les Données à caractère personnel. Les signalements réalisés en vertu de la présente section contiendront, dans la mesure possible, des informations concernant l'Incident touchant des données, y compris les mesures prises pour pallier les risques potentiels et les mesures qu'Esri recommande au Client de prendre eu égard à l'Incident touchant des données. Esri n'évaluera pas le contenu des Données à caractère personnel afin d'identifier les informations soumises à des exigences légales spécifiques. Le Client est le seul responsable du respect des lois applicables au Client en matière de signalement des incidents et du respect des obligations de signalement à des tiers liés à tout Incident touchant des données. Le signalement par Esri d'un Incident touchant des données ou la mesure prise par Esri en réponse à un Incident touchant des données en vertu de la présente section ne sera pas interprété(e) comme une reconnaissance par Esri de toute faute ou responsabilité dans le cadre de l'Incident touchant des données.
- C. Esri dispose actuellement des certifications et processus de contrôle de tiers, comme décrit sous <https://trust.arcgis.com>. Esri participe au cadre de confidentialité des données et a certifié sa conformité à celui-ci.
- D. Esri se conformera aux lois applicables en matière de protection et de confidentialité des données, y compris, sans toutefois s'y limiter, au RGPD et au CCPA, dans la mesure où ces lois s'appliquent à Esri en sa qualité de Sous-traitant ou de Prestataire de Services.
- E. Le Client certifie qu'il :
- i. a obtenu l'accord écrit, le consentement exprès ou une autre autorisation écrite (« **Consentement** ») auprès des personnes concernées ou dispose d'une autre base juridique légitime pour fournir ou rendre les Données à caractère personnel accessibles à Esri (ainsi qu'à ses filiales, sociétés affiliées et sous-traitants ultérieurs), et ce Consentement ou cette autre base juridique autorise Esri (et ses filiales, sociétés affiliées et sous-traitants ultérieurs) à traiter les Données à caractère personnel conformément aux dispositions du Contrat et du présent Addenda ; et
 - ii. s'est assuré que la fourniture et la communication des Données à caractère personnel à Esri sont conformes au RGPD, au CCPA et à toute autre Législation relative au respect de la vie privée qui s'appliquent au Client.
- F. Esri aidera le Client à s'assurer que ses obligations de traitement sécurisé, en qualité de Responsable du traitement, selon le RGPD sont remplies, ce qui peut inclure d'aider le Client dans une consultation avec une autorité de contrôle dans laquelle une analyse d'impact relative à la protection des données indique que le traitement prévu présenterait un niveau de risque élevé. Sur demande, Esri mettra à la disposition du Client les informations nécessaires pour démontrer le respect du RGPD et permettra la réalisation d'audits, y compris des inspections, et contribuera à ces audits pour confirmer la conformité d'Esri au présent Addenda par le Responsable du traitement ou un autre auditeur qu'il a mandaté. À la demande du Client aux fins de vérification, Esri fournira au Client un résumé de ses derniers résultats d'audit par un tiers indépendant ou de toute auto-évaluation similaire. Le résumé ne sera fourni qu'une fois par an, et la publication du résumé sera soumise à un accord écrit de non-divulcation entre les parties. Un audit sur site peut être effectué par le Client ou par un auditeur tiers indépendant, comme convenu par les parties dès lors que (i) un tel audit est requis par la Législation relative au respect de la vie privée ou par l'autorité de contrôle du Client compétente ; et (ii) le Client a reçu une notification d'Esri concernant un Incident touchant des Données à caractère personnel du Client. Le périmètre et l'horaire d'un tel audit seront mutuellement convenus à l'avance par les parties. Tout audit sur site sera limité aux infrastructures de traitement et de stockage des Contenus du Client exploitées par Esri. Le Client reconnaît qu'Esri exploite un environnement cloud

mutualisé. Par conséquent, Esri aura le droit d'adapter raisonnablement la portée de tout audit sur site pour éviter ou atténuer les risques concernant, notamment, les niveaux de service, la disponibilité et la confidentialité des informations des autres clients d'Esri. Toutes les dépenses résultant de cette sous-section F seront assumées par le Client, à moins qu'Esri ne soit jugé substantiellement non conforme. Le Client doit informer Esri de la découverte de toute non-conformité dans les plus brefs délais.

- G. Une fois que la finalité en vertu de laquelle le Client a fourni les Données à caractère personnel dans le cadre du présent Addenda, Esri devra renvoyer toutes les Données à caractère personnel traitées au nom du Client ou supprimer ou détruire les Données à caractère personnel, y compris les copies existantes, aux frais du Client, le cas échéant, à moins qu'Esri ne soit légalement tenu de conserver ces Données à caractère personnel.
- H. Les offres des Programmes de test, d'évaluation et Bêta peuvent utiliser des mesures de confidentialité et de sécurité inférieures ou différentes de celles généralement présentes dans les Online Services. Sauf indication contraire, le Client ne doit pas utiliser les offres de programmes de test, d'évaluation et Bêta pour traiter des Données à caractère personnel ou d'autres données soumises à des exigences de conformité légales ou réglementaires. Les conditions suivantes du présent Addenda ne s'appliquent pas aux offres des programmes de test, d'évaluation et Bêta : Traitement des Données à caractère personnel, RGPD, Sécurité des données et Partenaire commercial du Health Insurance Portability and Accountability Act (HIPAA).

LE CLIENT ATTESTE QU'IL COMPREND ET QUE SES COLLABORATEURS COMPRENNENT LES PRÉSENTES RESTRICTIONS ET QU'IL LES RESPECTERA.

EN FOI DE QUOI, les parties confirment leur accord sur ce qui précède lors de l'exécution en bonne et due forme du présent Addenda par leurs représentants autorisés respectifs. L'Addenda ne peut être modifié par aucune partie, sauf au moyen d'un document écrit distinct signé par les deux parties.

(Client)

Par : _____
Signature autorisée

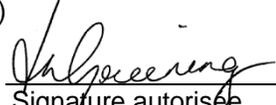
Nom en caractères d'imprimerie : _____

Poste : _____

Date : _____

Numéro de Client : _____

ENVIRONMENTAL SYSTEMS
RESEARCH INSTITUTE, INC.
(Esri)

Par :  _____
Signature autorisée

Nom en caractères d'imprimerie : Tamisa Greening

Poste : Directrice, service Contrats et juridique

ANNEXE 1
MISE EN ŒUVRE DES CLAUSES CONTRACTUELLES TYPES

1. Les Parties conviennent qu'en ce qui concerne la mise en œuvre des clauses contractuelles types de l'UE (décision 2021/914 de la Commission) (« CCT ») en vertu de l'Addendum, un ou plusieurs des Modules suivants des CCT s'appliqueront et sont référencés dans les présentes : (i) Responsable du traitement à Sous-traitant (« Module deux » ou « C2P ») ; (ii) Processeur à Processeur (« Module Trois » ou « P2P »).
2. Dans la mesure où une ou plusieurs des CTT ci-dessus s'appliquent, les Parties conviennent de ce qui suit :
 - a) La clause 7 (Clause d'adhésion) ne s'appliquera pas.
 - b) L'option 2 (Autorisation écrite générale) de la clause 9(a) (Recours à des sous-traitants ultérieurs) s'appliquera, et la période spécifique sera de trente (30) jours ;
 - c) L'option de la clause 11(a) (Voies de recours) ne s'appliquera pas ;
 - d) le droit applicable en vertu de la clause 17 (Droit applicable) sera le droit de la République d'Irlande ; et
 - e) la clause 18 (Élection de for et juridiction) désignera les tribunaux de la République d'Irlande.

ANNEXE I

A. LISTE DES PARTIES

Exportateur(s) de données :

1. **Nom** : Tel qu'identifié dans l'Accord et le présent Addenda

Adresse : Voir dossiers du Service Client d'Esri

Nom, fonction et coordonnées de la personne de contact : Voir dossiers du Service Client d'Esri

Activités en rapport avec les données transférées en vertu des présentes Clauses : Online Services et services d'abonnement et de maintenance fournis par Esri au Client

Signature et date : La signature par chaque partie de l'Addenda sera considérée comme une signature des présentes Clauses.

Rôle (responsable du traitement/sous-traitant) : Responsable du traitement

Importateur(s) de données :

1. **Nom** : Environmental Systems Research Institute, Inc. (« Esri »)

Adresse : 380 New York Street, Redlands, CA 92373, États-Unis

Nom, fonction et coordonnées de la personne de contact : Responsable de la sécurité des systèmes d'information, privacy@esri.com

Activités en rapport avec les données transférées en vertu des présentes Clauses : Online Services et services d'abonnement et de maintenance fournis par Esri au Client

Signature et date : La signature par chaque partie de l'Addenda sera considérée comme une signature des présentes Clauses.

Rôle (responsable du traitement/sous-traitant) : Sous-traitant

B. DESCRIPTION DU TRANSFERT

Catégories de personnes concernées dont les données à caractère personnel sont transférées

Les personnes dont les données sont fournies à Esri via les Online Services et les services d'abonnement et de maintenance par (ou sous la direction du) Client ou par les Utilisateurs finaux du Client, qui peuvent inclure les clients, les employés, les fournisseurs et les Utilisateurs finaux du Client.

Catégories de données à caractère personnel transférées

Les données relatives aux personnes sont fournies à Esri via les Online Services et les services d'abonnement et de maintenance par (ou sous la direction du) Client ou par les Utilisateurs finaux du Client.

Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

Considérant que seul le Client (et non Esri) a une connaissance et un contrôle complets sur les données fournies à Esri via les Online Services et les services d'abonnement et de maintenance, Esri traite tous les Contenus du Client conformément aux normes de données sensibles en appliquant les mesures techniques et organisationnelles décrites à l'Annexe II. Il incombe au Client de vérifier que ces mesures sont appropriées pour les catégories spécifiques de données fournies à Esri via les Online Services et les services d'abonnement et de maintenance.

Fréquence du transfert (indiquez, par exemple, si les données sont transférées sur une base ponctuelle ou continue).

La fréquence du transfert dépend de la fréquence à laquelle le Client fournit des Données à caractère personnel à Esri via les Online Services et les services d'abonnement et de maintenance. Il est prévu que les transferts puissent être ponctuels et/ou continus.

Nature du traitement

Analyse spatiale réalisée grâce aux opérations suivantes en fonction du choix du Client des paramètres et des actions effectuées : collecte, enregistrement, organisation, structuration, stockage, adaptation ou modification, récupération, consultation, utilisation, divulgation par transmission, diffusion ou mise à disposition, alignement ou combinaison, restriction, effacement ou destruction.

Finalité(s) du transfert et du traitement ultérieur de données

Esri traitera les Données à caractère personnel aux fins de fournir les Online Services et les services d'abonnement et de maintenance au Client conformément au Contrat.

Durée de conservation des données à caractère personnel, ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée

La période pendant laquelle les données à caractère personnel seront conservées dépend de la durée du traitement telle que déterminée par le Client et les instructions supplémentaires du Client.

Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement.

Cloud Services et services d'assistance technique impliquant des traitements de même nature et de même durée que ceux décrits ci-dessus.

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

Le cas échéant, toute autorité de contrôle compétente, conformément à la Clause 13

ANNEXE II

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

Esri mettra en place des garanties administratives, techniques et physiques pour préserver la sécurité, la confidentialité et l'intégrité des données à caractère personnel transmises dans le cadre des Services ArcGIS Online et des services d'abonnement et de maintenance, tels que décrits dans la Documentation relative à la sécurité et au respect de la vie privée applicable aux Services ArcGIS Online et aux services d'abonnement et de maintenance d'achetés par l'exportateur de données, telle que mise à jour à tout moment et accessible par l'intermédiaire du lien suivant <https://trust.arcgis.com/en/security/security-overview.htm> ou, de quelque manière que ce soit, mise à disposition de manière raisonnable par Esri.

A. Mesures techniques pour les Services ArcGIS Online. Esri a mis en œuvre les mesures techniques suivantes pour les Services ArcGIS Online référencés ci-dessus :

- i. L'algorithme de chiffrement de pointe et son paramétrage (par exemple, la longueur de la clé, le mode de fonctionnement, le cas échéant) sont utilisés pour les données Client stratégiques.
- ii. La puissance du chiffrement tient compte de la durée pendant laquelle la confidentialité des Données à caractère personnel cryptées doit être préservée.
- iii. L'algorithme de chiffrement est mis en œuvre par un logiciel dûment mis à jour dont la conformité à la spécification de l'algorithme choisi a été vérifiée par certification.
- iv. Les clés sont gérées de manière fiable (générées, administrées, stockées, liées à l'identité d'un destinataire prévu et révoquées).
- v. ArcGIS Online permet au Client (exportateur de données) de pseudonymiser les champs (par exemple, les informations d'identification de l'utilisateur) de manière à ce que les Données à caractère personnel ne puissent plus être attribuées à une personne concernée spécifique, ni être utilisées pour distinguer la personne concernée dans un plus grand groupe, sans l'utilisation d'informations supplémentaires détenues et contrôlées exclusivement par le Client (exportateur de données), dont le Client (exportateur de données) conserve le contrôle exclusif de l'algorithme ou du référentiel qui permet la réidentification à l'aide d'informations supplémentaires.
- vi. ArcGIS Online prend en charge les meilleures pratiques pour les protocoles de chiffrement de transport.
- vii. Une autorité et une infrastructure de certification à clé publique fiables sont utilisées.
- viii. Des mesures de protection spécifiques et de pointe sont utilisées contre les attaques actives et passives.
- ix. L'existence de moyens détournés (matériels ou logiciels) a été exclue.
- x. ArcGIS Online peut être utilisé en combinaison avec ArcGIS Enterprise dans une configuration qui permet au Client (exportateur de données) de stocker et de gérer des Données à caractère personnel sous le contrôle du Client (exportateur de données) sans les transférer vers un pays tiers, tandis qu'un exportateur de données traite les Données à caractère personnel dans de telle manière qu'elles sont divisées en deux ou plusieurs parties, et la partie qui est transférée vers le pays tiers ne peut plus être interprétée ou attribuée à une personne concernée spécifique sans l'utilisation d'informations supplémentaires sous le contrôle du Client (exportateur de données).

Des informations supplémentaires sur les mesures techniques peuvent être trouvées à l'adresse : <https://trust.arcgis.com/en/documents/>

B. Mesures organisationnelles et contractuelles

- i. Les efforts d'Esri en matière de confidentialité sont décrits sur la page <https://www.esri.com/en-us/privacy/overview>.
- ii. Esri s'engage à traiter les Données à caractère personnel conformément à sa Déclaration de confidentialité (disponible à l'adresse : <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>) et au Supplément à la déclaration de confidentialité des produits et services Esri (disponible à l'adresse : <https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement>).
- iii. Esri fournit ici un Addenda sur le traitement des données présigné qui contient les Clauses contractuelles types, disponible à l'adresse : <https://www.esri.com/en-us/privacy/privacy-gdpr>.

- iv. Esri maintient et applique une politique interne de protection des informations personnelles qui oblige les employés à protéger les Données à caractère personnel auxquelles ils accèdent.
- v. Esri maintient une politique de sécurité d'entreprise qui propose des contrôles d'accès et des mesures de sécurité d'entreprise.

C. Adoption d'exigences supplémentaires et Droit à une Résiliation anticipée. Si les autorités de contrôle adoptent d'autres exigences et mesures concernant le transfert de données à caractère personnel vers les États-Unis, Esri modifiera le présent Addenda afin de répondre aux exigences supplémentaires. Si Esri ne peut pas répondre aux exigences supplémentaires, le Client aura le droit de résilier le Contrat à sa convenance (sans frais de résiliation ni pénalité) en informant Esri par écrit.