

Dieser Anhang zur Datenverarbeitung („**Anhang**“) gilt ab dem ersten Tag, an dem der Kunde Esri personenbezogene Daten (wie im Folgenden definiert) zur Verfügung stellt, die geltenden Datenschutzgesetzen (wie im Folgenden definiert) unterliegen. Dieser Anhang ist Teil der Lizenzvereinbarung oder einer anderen schriftlichen oder elektronischen Vereinbarung („**Vereinbarung**“) zwischen der Organisation, die nachstehend unterzeichnet oder zustimmt („**Kunde**“), und dem **Environmental Systems Research Institute, Inc.** („**Esri**“). Dieser Anhang definiert die Bedingungen für den Datenschutz, die Vertraulichkeit und die Sicherheit personenbezogener Daten im Zusammenhang mit den Online-Diensten sowie den Abonnement- und Wartungsdiensten, die von Esri für den Kunden gemäß der Vereinbarung erbracht werden. Alle in der Vereinbarung definierten oder verwendeten Begriffe haben, sofern nicht anderweitig definiert, in diesem Anhang dieselbe Bedeutung. In diesem Anhang verwendete Begriffe, die weder hier noch in der Vereinbarung definiert sind, haben die im geltenden Datenschutzgesetz festgelegte Bedeutung.

Da der Kunde Esri, einem in den USA ansässigen Unternehmen, Zugriff auf personenbezogene Daten gewähren kann, damit Esri als Auftragsverarbeiter oder Service-Provider diese im Zusammenhang mit Online-Diensten sowie Abonnement- und Wartungsdiensten für den Kunden gemäß der Vereinbarung verarbeitet; und

da der Kunde wünscht, dass Esri als Auftragsverarbeiter den Datenschutz und die Sicherheit dieser personenbezogenen Daten gemäß den Bestimmungen dieses Anhangs wahrt und aufrechterhält,

vereinbaren Esri und der Kunde unter Berücksichtigung der gemeinsamen Zusicherungen und Vereinbarungen in diesem Anhang und in der Vereinbarung sowie aus anderen triftigen und gerechtfertigten Gründen, deren Hinlänglichkeit hiermit anerkannt wird, Folgendes:

ABSCHNITT I – DEFINITIONEN

- A. „**Datenschutzgesetz**“ bezeichnen die Datenschutz-Grundverordnung (DSGVO) der EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, den California Consumer Privacy Act von 2018 (CCPA) (in der durch den California Privacy Rights Act [CPRA] geänderten Fassung) sowie sonstige für Esri geltende Datenschutzgesetze.
- B. Die in diesem Anhang verwendeten Begriffe „personenbezogene Daten“, „betroffene Person“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“ und „Aufsichtsbehörde“ haben die in der Datenschutz-Grundverordnung festgelegte Bedeutung.
- C. „**Personenbezogene Daten**“ sind personenbezogene Daten, persönliche Informationen oder persönlich identifizierbare Informationen gemäß der Definition in den geltenden Datenschutzgesetzen über Personen, die in der Europäischen Union, der Schweiz, dem Vereinigten Königreich, Kalifornien, USA, oder an anderen Orten ansässig sind, an denen Datenschutzgesetze gelten. Personenbezogene Daten können unter anderem Folgendes beinhalten: (i) Kategorien von betroffenen Personen: Interessenten, Kunden, Geschäftspartner und Lieferanten und (ii) Arten von personenbezogenen Daten: Name, Titel, Position, E-Mail-Adresse und Standort.
- D. „**Datenvorfall**“ bezeichnet eine Verletzung der Sicherheitsmaßnahmen von Esri, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von oder zum Zugriff auf personenbezogene Daten in Systemen führt, die von Esri verwaltet oder anderweitig kontrolliert werden. Datenvorfälle umfassen keine erfolglosen Versuche oder Handlungen, die die Sicherheit personenbezogener Daten nicht beeinträchtigen, einschließlich erfolgloser Anmeldeversuche, Pings, Port-Scans, Denial-of-Service-Angriffe und anderer Netzwerkangriffe auf Firewalls oder vernetzte Systeme.

ABSCHNITT II – DATENSCHUTZ, VERTRAULICHKEIT UND DATENSICHERHEIT

- A. Berechtigung zur Verarbeitung personenbezogener Daten
 - i. Der Kunde und Esri stimmen darin überein, dass der Kunde als Verantwortlicher und Esri als Auftragsverarbeiter oder Service-Provider von personenbezogenen Daten agieren; sofern nicht der Kunde ein Auftragsverarbeiter von personenbezogenen Daten ist, denn in diesem Fall ist Esri ein Unterauftragsverarbeiter.

- ii. Die Bestimmungen dieses Anhangs gelten nicht, wenn Esri als Verantwortlicher für die personenbezogenen Daten agiert (z. B. personenbezogene Daten, die zwecks Kontoeinrichtung, Autorisierung und Anmeldung bei Konten von Esri empfangen und verarbeitet wurden). Wenn Esri der Verantwortliche ist, finden die Esri Datenschutzbestimmungen (hier verfügbar: <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>) sowie alle dazugehörigen Datenschutzhinweise oder -erklärungen und die Vereinbarung zur Datenübertragung Anwendung.
- iii. Esri verarbeitet personenbezogene Daten nur nach schriftlicher Anweisung des Kunden (a) für und zugunsten des Kunden, (b) zum Zweck der Verarbeitung personenbezogener Daten im Zusammenhang mit der Vereinbarung und (c) zur Erfüllung seiner Pflichten gemäß dieses Anhangs, der Vereinbarung und der geltenden Datenschutzgesetze sowie anderer Gesetze.
- iv. Der Kunde verfügt über die ausschließliche Berechtigung, über die Zwecke und Mittel für die Verarbeitung von personenbezogenen Daten zu entscheiden. Esri wird (a) personenbezogene Daten nicht außerhalb der direkten Geschäftsbeziehung zwischen den Parteien oder zu einem anderen Zweck als zur Erfüllung der Vereinbarung speichern, verwenden oder offenlegen, außer insoweit dies nach diesem Anhang oder den Datenschutzgesetzen zulässig ist; und (b) wird die personenbezogenen Daten des Kunden nicht mit anderen personenbezogenen Daten kombinieren, die von oder im Namen einer anderen Person erhalten oder erhoben wurden; dies gilt vorausgesetzt, dass Esri personenbezogene Daten für einen geschäftlichen Zweck (gemäß der Definition in CCPA/CPRA) kombinieren darf.
- v. Gegenstand und Einzelheiten der Verarbeitung werden in Annex I zu Anlage 1 beschrieben, und dieser Anhang (einschließlich der Anlage und der Annexe) sowie die Vereinbarung stellen die vollständigen Anweisungen des Kunden an Esri hinsichtlich der Verarbeitung von personenbezogenen Daten dar. Jegliche anderweitigen oder zusätzlichen Anweisungen sind nur als schriftliche Ergänzung dieses Anhangs möglich.
- vi. Insofern der Kunde Esri anonymisierte Daten (wie in CCPA/CPRA oder in sonstigen Datenschutzgesetzen definiert) offenlegt oder anderweitig zur Verfügung stellt oder Esri anonymisierte Daten aus personenbezogenen Daten erstellt, wird Esri (a) angemessene Maßnahmen ergreifen, um sicherzustellen, dass diese anonymisierten Daten nicht dazu verwendet werden, Informationen über eine bestimmte natürliche Person oder einen bestimmten Haushalt herzuleiten oder anderweitig damit assoziiert zu werden; (b) sich öffentlich dazu verpflichten, solche anonymisierten Daten in anonymisierter Form aufzubewahren und zu verwenden und nicht zu versuchen, die anonymisierten Daten erneut zu identifizieren; und (c) vor der Weitergabe anonymisierter Daten an verbundene Unternehmen oder Dritte, einschließlich Unterauftragsverarbeitern, Auftragnehmern oder anderen Personen („Empfänger“), diese Empfänger vertraglich verpflichten, alle Anforderungen dieses Abschnitts einzuhalten. Ungeachtet des vorstehenden Satzes kann Esri versuchen, die Daten ausschließlich zu dem Zweck erneut zu identifizieren, um festzustellen, ob seine Anonymisierungsverfahren mit den Datenschutzgesetzen konform sind.

B. Offenlegung von und Zugriff auf personenbezogene Daten

- i. Esri behandelt alle personenbezogenen Daten vertraulich. Esri wird personenbezogene Daten weder verkaufen noch weitergeben (wie im CCPA/CPRA definiert).
- ii. Esri (a) bietet für die vom Kunden erhaltenen personenbezogenen Daten mindestens jenen Grad an Datenschutz, der von der DSGVO, dem CCPA und den anderen geltenden Datenschutzgesetzen gefordert wird, (b) benachrichtigt den Kunden stets umgehend, falls Esri feststellt, dass Esri nicht mehr länger in der Lage ist, den datenschutzrechtlich geforderten Grad an Datenschutz zu bieten. Wenn der Kunde Esri zu irgendeinem Zeitpunkt auf seinen begründeten Verdacht hinweist, dass Esri die personenbezogenen Daten nicht gemäß den Datenschutzgesetzen verarbeitet, kann der Kunde angemessene und geeignete Schritte unternehmen, um die unbefugte Verarbeitung dieser personenbezogenen Daten zu stoppen und zu beheben.
- iii. Falls Esri vom Kunden zur Verfügung gestellte personenbezogene Daten verarbeitet, die der DSGVO unterliegen und Esri in einem Land ansässig ist oder personenbezogene Daten an Unterauftragsverarbeiter in einem Land übermittelt oder zugänglich macht, das keine angemessenen Datenschutzvorkehrungen gemäß der DSGVO vorsieht, wird Esri mit dem Kunden die Standardvertragsklauseln („SVK“) gemäß Anlage 1 zu diesem Anhang abschließen. Falls zutreffend, gilt die Unterzeichnung dieses Anhangs zur Datenverarbeitung durch jede Partei als Unterzeichnung der SVK. Falls ein Unterauftragsverarbeiter ein Datenimporteur ist (wie dieser Begriff in diesen SVK gemäß der DSGVO verwendet wird), hat Esri entweder (a) vertragliche Pflichten mit dem Unterauftragsverarbeiter zu vereinbaren, wobei diese Pflichten

- angemessene Datenschutzmaßnahmen gemäß der DSGVO enthalten, oder (b) die Standardvertragsklauseln mit dem Kunden im Namen dieses Datenimporteurs abzuschließen.
- iv. Esri wird personenbezogene Daten weder an Dritte weitergeben, übermitteln, offenlegen oder einen anderweitigen Zugriff ermöglichen noch seine Rechte und Pflichten im Hinblick auf personenbezogene Daten vertraglich auf Dritte übertragen, es sei denn, der Kunde hat Esri dazu schriftlich berechtigt oder es besteht eine gesetzliche Pflicht. Sofern Esri mit Zustimmung des Kunden Dritten Zugriff auf personenbezogene Daten gewährt oder entsprechende Rechte und Pflichten vertraglich auf Dritte überträgt, (a) schließt Esri mit dem jeweiligen Dritten eine schriftliche Vereinbarung ab, die diesen zur Einhaltung der DSGVO, des CCPA und der sonstigen Datenschutzgesetze verpflichtet, (b) übermittelt Esri die personenbezogenen Daten nur für den eingeschränkten und angegebenen Zweck, gemäß Instruktionen des Kunden, (c) fordert Esri von diesem Dritten, dass er Esri in Kenntnis setzt, falls er nicht mehr länger in der Lage ist, den durch geltende Datenschutzgesetze geforderten Grad des Datenschutzes aufrechtzuerhalten, und (d) verpflichtet Esri diesen Dritten, auf entsprechenden Hinweis hin, angemessene und geeignete Schritte zu unternehmen, eine nicht berechtigte Verarbeitung zu beenden und zu berichtigen. Der Kunde erteilt hiermit seine Einwilligung, dass Esri die für die Erfüllung seiner Leistungen erforderlichen Unterauftragsverarbeiter wie z. B. Microsoft Corporation, Amazon Web Services Inc., Salesforce, Inc.; Akamai Technologies (einschließlich verbundener Unternehmen) und die Anbieter von Technischem Support von Esri einsetzen darf. Wenn Esri andere Unterauftragsverarbeiter einsetzt, wird Esri den Kunden informieren und ihm ein Einspruchsrecht einräumen. Legt der Kunde einen begründeten Einspruch gegen die Änderung der Unterauftragsverarbeiter ein, muss dieser von den Parteien in angemessener Weise geklärt werden.
 - v. Esri wird den Kunden umgehend schriftlich über jegliche Anfragen in Bezug auf die personenbezogenen Daten informieren, die Esri von Kunden, Verbrauchern, Mitarbeitern oder anderen Partnern des Kunden erhält. Der Kunde ist für die Ergreifung von Maßnahmen sowie für die Beantwortung dieser Anfragen verantwortlich. Esri wird jedoch angemessen mit dem Kunden zusammenarbeiten, um derartige Anfragen zu klären. Dies gilt auch für Anfragen natürlicher Personen, deren personenbezogene Daten zwecks Zugriffs, Berichtigung, Widerspruchs, Übertragbarkeit, Beschränkung, Löschung oder Exports von Esri vorgehalten werden. Klarstellend wird angemerkt, dass der Kunde, wie in der Lizenzvereinbarung definiert, als Verantwortlicher für die Named-User-Credentials gilt. Der Kunde ist allein für die Ergreifung von Maßnahmen sowie für die Beantwortung aller Anfragen betroffener Personen im Zusammenhang mit Named-User-Credentials verantwortlich.
 - vi. Unter Berücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen wird Esri geeignete technische und organisatorische Maßnahmen ergreifen, um die personenbezogenen Daten von EU-Bürgern vor Verlust, Missbrauch sowie unberechtigtem Zugriff, Offenlegung, Veränderung und Zerstörung zu schützen. Diese Maßnahmen sind in Annex II zu Anlage 1 dargelegt. Zu diesem Zweck beschränkt Esri den internen Zugriff auf die personenbezogenen Daten dahingehend, dass dieser nur dann gewährt wird, wenn er zur Erbringung der Dienstleistungen von Esri für oder zugunsten des Kunden für die Mitarbeiter erforderlich ist, die Datenschutz- und Sicherheitsauflagen zugestimmt haben, welche den Anforderungen dieses Anhangs grundsätzlich ähneln.
 - vii. Gemäß geltendem Recht wird Esri den Kunden umgehend schriftlich von jeglichen Vorladungen oder anderen gerichtlichen oder behördlichen Anordnungen sowie Verfahren in Kenntnis setzen, die einen Zugriff auf oder eine Offenlegung von personenbezogenen Daten anstreben. Der Kunde kann nach eigenem Ermessen eine einstweilige Verfügung erwirken und Esri wird auf angemessene Weise mit dem Kunden an einer solchen Maßnahme mitwirken, sofern der Kunde Esri sämtliche dadurch entstehenden Kosten, Gebühren und Honorare erstattet. Esri ist berechtigt, jegliche Einigungen zu billigen oder abzulehnen, die Esri betreffen.
 - viii. Sofern Esri von einem Datenvorfall Kenntnis erlangt, wird Esri (a) den Kunden nach Kenntnis unverzüglich und ohne unangemessene Verzögerung über den Datenvorfall informieren, und (b) unverzüglich angemessene Maßnahmen ergreifen, um den Schaden zu minimieren und die personenbezogenen Daten zu schützen. Die gemäß diesem Abschnitt vorgenommenen Benachrichtigungen beschreiben, soweit möglich, Einzelheiten des Datenvorfalles, einschließlich der Maßnahmen zur Minderung der potenziellen Risiken und der Maßnahmen, die Esri dem Kunden empfiehlt, um den Datenvorfall zu beheben. Esri wird keine Bewertung der Inhalte der personenbezogenen Daten vornehmen, um Informationen zu ermitteln, die besonderen gesetzlichen Anforderungen unterliegen. Der Kunde ist allein verantwortlich für die

Einhaltung der für den Kunden geltenden Gesetze zur Benachrichtigung über Vorfälle und die Erfüllung aller Benachrichtigungspflichten gegenüber Dritten im Zusammenhang mit einem Datenvorfall bzw. mit Datenvorfällen. Die Benachrichtigung von Esri über oder die Reaktion auf einen Datenvorfall in diesem Abschnitt gilt nicht als Bestätigung von Esri über einen Fehler oder eine Haftung in Bezug auf den Datenvorfall.

- C. Esri verfügt derzeit über die unter <https://trust.arcgis.com> beschriebenen Prüfverfahren und Zertifizierungen von Dritten.
- D. Esri hält sich an geltende Datenschutzgesetze, insbesondere die DSGVO und das CCPA, insoweit diese für Esri als Auftragsverarbeiter oder Service-Provider gelten.
- E. Der Kunde bestätigt:
 - i. dass er eine schriftliche Einwilligung, Bejahung oder andere schriftliche Berechtigung („**Einwilligung**“) der betreffenden Personen erhalten hat oder über eine andere zulässige, rechtmäßige Grundlage verfügt, um Esri (sowie seinen Tochterunternehmen, angeschlossenen Unternehmen und Unterauftragsverarbeitern) personenbezogene Daten zur Verfügung zu stellen oder zugänglich zu machen, und dass diese Einwilligung oder anderweitige rechtmäßige Grundlage es Esri (sowie seinen Tochterunternehmen, angeschlossenen Unternehmen und Unterauftragsverarbeitern) gestattet, die personenbezogenen Daten unter Einhaltung der Bestimmungen der Vereinbarung sowie dieses Anhangs zu verarbeiten; und
 - ii. dass er sichergestellt hat, dass die Bereitstellung und Offenlegung personenbezogener Daten an Esri in Übereinstimmung mit der DSGVO, dem CCPA und den sonstigen, für den Kunden geltenden, Datenschutzgesetzen erfolgen.
- F. Esri wird den Kunden als Verantwortlichen darin unterstützen, seiner Pflicht zur sicheren Verarbeitung im Sinne der DSGVO nachzukommen. Dies kann die Unterstützung des Kunden bei Anhörungen durch eine Aufsichtsbehörde einschließen, wenn eine Datenschutz-Folgenabschätzung ergibt, dass die beabsichtigte Verarbeitung zu einem hohen Risiko führen würde. Esri wird dem Kunden auf Anforderung alle Informationen zur Verfügung stellen, die für den Nachweis der Einhaltung der DSGVO erforderlich sind. Esri wird Überprüfungen – einschließlich Inspektionen – ermöglichen und an diesen mitwirken, damit die Einhaltung dieses Anhangs seitens Esri durch den Verantwortlichen oder einen von diesem beauftragten Prüfer nachgewiesen werden kann. Auf Verlangen des Kunden zur Bestätigung der Einhaltung wird Esri dem Kunden eine Zusammenfassung der Ergebnisse der letzten Prüfung durch einen unabhängigen Dritten oder eine gleichwertige Selbstbeurteilung zur Verfügung stellen. Die Zusammenfassung erfolgt nicht öfter als einmal jährlich und die Offenlegung der Zusammenfassung unterliegt einer schriftlichen Geheimhaltungsvereinbarung der Parteien. Durch den Kunden oder einen durch die Parteien gemeinsam benannten unabhängigen Prüfer kann eine Prüfung vor Ort durchgeführt werden, wenn (i) die Prüfung durch Datenschutzgesetze oder die zuständige Aufsichtsbehörde des Kunden vorgeschrieben ist, und (ii) der Kunde eine Mitteilung von Esri über einen Datenvorfall erhalten hat, der die personenbezogenen Daten des Kunden betrifft. Umfang und die zeitliche Planung einer solchen Prüfung werden von den Parteien im Voraus einvernehmlich festgelegt. Alle Prüfungen vor Ort beschränken sich auf die von Esri betriebenen Einrichtungen zur Verarbeitung und Speicherung von Kundeninhalten. Der Kunde bestätigt, dass Esri eine mandantenfähige Cloud-Umgebung betreibt. Esri ist daher berechtigt, den Umfang einer Prüfung vor Ort in angemessener Weise anzupassen, um Risiken in Bezug auf Service-Level, Verfügbarkeit und Vertraulichkeit der Informationen anderer Esri Kunden zu vermeiden oder zu mindern. Alle Ausgaben im Zusammenhang mit diesem Unterabschnitt F sind vom Kunden zu tragen, sofern Esri nicht ein erheblicher Verstoß nachgewiesen wird. Der Kunde muss Esri unverzüglich über jede festgestellte Nichteinhaltung informieren.
- G. Nach Erreichung des Zwecks, für den der Kunde die personenbezogenen Daten unter diesem Anhang zur Verfügung gestellt hat, gibt Esri entweder alle zugunsten des Kunden verarbeiteten personenbezogenen Daten zurück oder löscht oder zerstört diese auf Kosten des Kunden, einschließlich aller ggf. vorhandenen Kopien, es sei denn, Esri ist gesetzlich dazu verpflichtet, derartige personenbezogene Daten aufzubewahren.

H. Test-, Evaluierungs- und Betaprogrammangebote können weniger oder andere Datenschutz- und Sicherheitsmaßnahmen als die in den Online-Diensten üblichen verwenden. Sofern nicht etwas anderes angegeben ist, sollte der Kunde keine Test-, Evaluierungs- und Betaprogrammangebote zur Verarbeitung von personenbezogenen oder andere Daten nutzen, die gesetzlichen oder behördlichen Anforderungen zur Einhaltung unterliegen. Die folgenden Begriffe in diesem Anhang gelten nicht für Test-, Evaluierungs- und Betaprogrammangebote: Verarbeitung personenbezogener Daten, DSGVO, Datensicherheit und Health Insurance Portability and Accountability Act (HIPAA) Business Associate.

DER KUNDE BESTÄTIGT, DASS ER UND SEINE MITARBEITER DIESE EINSCHRÄNKUNGEN VERSTEHEN UND BEFOLGEN WERDEN.

ZUM ZEUGNIS DESSEN bestätigen die Parteien ihre Zustimmung zum Vorangehenden durch ordnungsgemäße Ausfertigung dieses Anhangs durch ihre jeweils bevollmächtigten Vertreter. Dieser Anhang darf durch die Parteien nur mittels eines gesonderten und durch beide Parteien unterzeichneten Schriftstücks geändert oder ergänzt werden.

(Kunde)

Unterzeichnet von: _____
Bevollmächtigter (Unterschrift)

Name (Druckschrift): _____

Titel: _____

Datum: _____

Kundennummer: _____

ENVIRONMENTAL SYSTEMS
RESEARCH INSTITUTE, INC.
(Esri)

Unterzeichnet von: 
Bevollmächtigter (Unterschrift)

Name (Druckschrift): Tamisa Greening

Titel: Director, Contracts and Legal

ANLAGE 1
UMSETZUNG DER STANDARDVERTRAGSKLAUSELN

1. Die Parteien kommen überein, dass für die Umsetzung der Standardvertragsklauseln im Rahmen des Anhangs eines oder mehrere der folgenden Module der Standardvertragsklauseln gelten, auf die hier Bezug genommen wird: (i) Verantwortlicher an Auftragsverarbeiter („Modul Zwei“ oder „C2P“); (ii) Auftragsverarbeiter an Auftragsverarbeiter („Modul Drei“ oder „P2P“).
2. Insofern eine oder mehrere der vorgenannten Standardvertragsklauseln Anwendung finden, vereinbaren die Parteien Folgendes:
 - a) Klausel 7 (Kopplungsklausel) findet keine Anwendung;
 - b) Option 2 (Allgemeine schriftliche Genehmigung) von Klausel 9(a) (Einsatz von Unterauftragsverarbeitern) findet Anwendung, und die Frist beträgt dreißig (30) Tage;
 - c) Klausel 11(a) (Rechtsbehelf) findet keine Anwendung;
 - d) Anwendbares Recht gemäß Klausel 17 (Anwendbares Recht) ist das Recht der Republik Irland; und
 - e) Klausel 18 (Wahl des Gerichtsstands und der Gerichtsbarkeit) bezieht sich auf die Gerichte der Republik Irland.

ANNEX I

A. LISTE DER PARTEIEN

Datenexporteur(e):

1. **Name:** Wie in der Vereinbarung und diesem Anhang angegeben

Adresse: Gemäß der Esri Kundendatensätze

Name, Position und Kontaktdaten der Kontaktperson: Gemäß der Esri Kundendatensätze

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Online-Dienste sowie Abonnement- und Wartungsdienste, die von Esri für den Kunden erbracht werden

Unterschrift und Datum: Die Unterzeichnung des Anhangs durch jede Partei gilt als Unterzeichnung dieser Klauseln.

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Datenimporteur(e):

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

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

Name, Position und Kontaktdaten der Kontaktperson: Chief Information Security Officer,
privacy@esri.com

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Online-Dienste sowie Abonnement- und Wartungsdienste, die von Esri für den Kunden erbracht werden

Unterschrift und Datum: Die Unterzeichnung des Anhangs durch jede Partei gilt als Unterzeichnung dieser Klauseln.

Rolle (Verantwortlicher/Auftragsverarbeiter): Auftragsverarbeiter

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

Daten zu natürlichen Personen, über die Esri durch die Online-Dienste und Abonnement- und Wartungsdienste des Kunden (oder auf Anweisung des Kunden) oder von Endbenutzern des Kunden Daten zur Verfügung gestellt werden, zu denen Kunden, Mitarbeiter, Lieferanten und Endbenutzer des Kunden gehören können.

Kategorien der übermittelten personenbezogenen Daten

Daten zu natürlichen Personen, über die Esri durch die Online-Dienste und Abonnement- und Wartungsdienste des Kunden (oder auf Anweisung des Kunden) oder von Endbenutzern des Kunden Daten zur Verfügung gestellt werden.

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

In Anbetracht der Tatsache, dass nur der Kunde (und nicht Esri) die volle Kenntnis und Kontrolle darüber hat, welche Daten Esri über die Online-Dienste und die Abonnement- und Wartungsdienste zur Verfügung gestellt werden, behandelt Esri alle Kundeninhalte gemäß den Standards für sensible Daten, indem es die in Annex II beschriebenen technischen und organisatorischen Maßnahmen bereitstellt. Der Kunde ist dafür verantwortlich, zu überprüfen, ob diese Maßnahmen für die spezifischen Datenkategorien, die Esri über die Online-Dienste und die Abonnement- und Wartungsdienste zur Verfügung gestellt werden, angemessen sind.

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)

Die Häufigkeit der Übermittlung hängt von der Häufigkeit ab, mit der der Kunde Esri personenbezogene Daten über die Online-Dienste und Abonnement- und Wartungsdienste zur Verfügung stellt. Es wird davon ausgegangen, dass es sich um einmalige und/oder kontinuierliche Übertragungen handelt.

Art der Verarbeitung

Die räumliche Analyse erfolgt durch folgende Vorgänge, die von den vom Kunden gewählten Einstellungen und durchgeführten Aktionen abhängen: Erfassung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, Abruf, Abfrage, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Methode von Bereitstellung, Abgleich oder Kombination, Einschränkung, Löschung oder Vernichtung.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Esri verarbeitet personenbezogene Daten zum Zwecke der Erbringung der Online-Dienste sowie der Abonnements- und Wartungsleistungen für den Kunden in Übereinstimmung mit der Vereinbarung.

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Die Dauer, für die die personenbezogenen Daten gespeichert werden, hängt von der Dauer der Verarbeitung ab, die vom Kunden und seinen zusätzlichen Anweisungen bestimmt wird.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

Cloud-Dienste und Technischer Support umfassen die Verarbeitung der gleichen Art und Dauer wie vorstehend beschrieben wird.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13.

ANNEX II TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH JENER ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Esri unterhält administrative, physische und technische Sicherheitsvorkehrungen zum Schutz der Sicherheit, Vertraulichkeit und Integrität der auf ArcGIS Online Services und Abonnement- und Wartungsdienste hochgeladenen personenbezogenen Daten, wie in der Sicherheits- und Datenschutzdokumentation beschrieben, die für die spezifischen ArcGIS Online Services und Abonnement- und Wartungsdienste gilt, die der Datenexporteur erworben hat, und die von Zeit zu Zeit aktualisiert wird und über <https://trust.arcgis.com/en/security/security-overview.htm> zugänglich ist oder anderweitig von Esri in angemessener Weise bereitgestellt wird.

A. Technische Maßnahmen für ArcGIS Online Services. Esri hat die folgenden, technischen Maßnahmen für die oben genannten ArcGIS Online Services durchgeführt:

- i. Der moderne Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, Betriebsmodus, falls anwendbar) werden für inaktive Kundendaten verwendet.
- ii. Die Stärke der Verschlüsselung berücksichtigt den Zeitraum, während dem die Vertraulichkeit der verschlüsselten Daten sichergestellt werden muss.
- iii. Der Verschlüsselungsalgorithmus wird durch eine entsprechend aktualisierte Software implementiert, deren Konformität zur Spezifikation des gewählten Algorithmus durch die Zertifizierung überprüft wurde.
- iv. Die Schlüssel werden sicher verwaltet (erzeugt, administriert, gespeichert, zur Identifizierung an den vorgesehenen Empfänger gebunden und annulliert).
- v. ArcGIS Online erlaubt es dem Kunden (Datenexporteur), die Felder derart zu pseudonymisieren (z. B. Benutzerzugangsdaten), dass die personenbezogenen Daten weder einer spezifischen betroffenen Person zuzuordnen noch verwendbar sind, um die betroffene Person aus einer größeren Gruppe auszuwählen, ohne dass dafür weitere Informationen erforderlich wären, über deren Algorithmus oder Aufbewahrungsort, die eine erneute Identifizierung unter Verwendung der zusätzlichen Informationen ermöglichen, ausschließlich der Kunde (Datenexporteur) die Kontrolle besitzt.
- vi. ArcGIS Online unterstützt die Best Practices für die Übertragung von Verschlüsselungsprotokollen.
- vii. Eine vertrauenswürdige Zertifizierungsstelle und Infrastruktur für öffentliche Schlüssel werden eingesetzt.
- viii. Spezielle hochmoderne Maßnahmen werden zum Schutz gegen aktive und passive Angriffe ergriffen.
- ix. Die Existenz von Hintertüren (bei Hard- oder Software) wurde ausgeschlossen.
- x. ArcGIS Online kann zusammen mit ArcGIS Enterprise in einer Konfiguration verwendet werden, die es dem Kunden (Datenexporteur) erlaubt, personenbezogene Daten unter Aufsicht des Kunden (Datenexporteurs) zu speichern und zu verwalten, ohne diese in ein anderes Land zu übertragen, während ein Datenexporteur die personenbezogenen Daten auf eine Weise bearbeitet, dass er diese in zwei oder mehrere Teile aufteilt. Dabei kann der Teil, der in ein drittes Land übertragen wird, keiner bestimmten, betroffenen Person mehr zugeordnet werden, ohne dafür weitere Informationen zu haben, die sich unter der Kontrolle des Kunden (Datenexporteurs) befinden.

Weitere Informationen über technische Maßnahmen finden Sie hier: <https://trust.arcgis.com/en/documents/>.

B. Organisatorische und vertragliche Maßnahmen

- i. Die Bemühungen von Esri um den Datenschutz sind beschrieben unter <https://www.esri.com/en-us/privacy/overview>.
- ii. Esri verpflichtet sich, personenbezogene Daten gemäß seiner Datenschutzbestimmung (hier verfügbar: <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>) und dem Esri Products & Services Privacy Statement Supplement (hier verfügbar: <https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement>) zu behandeln.
- iii. Esri stellt einen bereits unterzeichneten Anhang zur Datenverarbeitung zur Verfügung, der Standardvertragsklauseln enthält: <https://www.esri.com/en-us/privacy/privacy-gdpr>.
- iv. Esri ergreift interne Sicherheitsmaßnahmen für personenbezogene Daten, die von den Angestellten verlangt, die personenbezogenen Daten zu schützen, auf die sie zugreifen.
- v. Esri pflegt eine Unternehmenssicherheitspolitik, die Zugriffskontrollen und Sicherheitsmaßnahmen des Unternehmens regelt.

C. Annahme weiterer Anforderungen und Recht auf vorzeitige Kündigung. Wenn Aufsichtsbehörden weitere Anforderungen und Maßnahmen in Bezug auf die Übermittlung personenbezogener Daten in die USA erlassen, wird Esri diesen Anhang ändern, um die zusätzlichen Anforderungen zu erfüllen. Wenn Esri die zusätzlichen Bedingungen nicht erfüllen kann, ist der Kunde dazu berechtigt, diese Vereinbarung aus praktischen Gründen (ohne Aufhebungs- oder Strafgebühr) durch schriftliche Benachrichtigung an Esri kündigen.