

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 Nachtrag 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, Informationen über Personen oder persönlich zuordenbare Daten gewähren kann, damit Esri als Auftragsverarbeiter oder Dienstleister 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 aufrecht erhält;

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. „**Datenschutzgesetze**“ bezeichnen die Datenschutz-Grundverordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, den California Consumer Privacy Act von 2018 sowie sonstige für Esri geltende Datenschutzgesetze.
- B. Die in diesem Nachtrag verwendeten Begriffe „personenbezogene Daten“, „betroffene Person“, „Verarbeitung“, „für die 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 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 an Konten von Esri empfangen und verarbeitet wurden).
- 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 Nachtrags, 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.
- v. Der Gegenstand und die Einzelheiten der Verarbeitung werden in Nachtrag 1 von Anhang 1 beschrieben, und dieser Anhang (einschließlich des Nachtrags) 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.

B. Offenlegung von und Zugriff auf personenbezogene Daten

- i. Esri behandelt alle personenbezogenen Daten vertraulich. Esri verkauft keine personenbezogene Daten.
- 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 von den Datenschutzgesetzen geforderten Grad an Datenschutz zu bieten, und (c) unternimmt angemessene und geeignete Schritte, die Verarbeitung von solchen personenbezogenen Daten immer dann zu berichtigen, wenn der Kunde Esri auf seinen begründeten Verdacht hinweist, dass Esri die personenbezogenen Daten nicht gemäß den Datenschutzgesetzen verarbeitet.
- 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 gemäß Nachtrag 1 dieses Anhangs abschließen. Falls zutreffend, gilt die Unterzeichnung dieses Anhangs zur Datenverarbeitung durch jede Partei als Unterzeichnung der Standardvertragsklauseln (einschließlich der Anhänge und Nachträge). Falls ein Unterauftragsverarbeiter ein Datenimporteur ist (wie dieser Begriff in diesen Standardvertragsklauseln gemäß der DSGVO verwendet wird), hat Esri entweder (a) vertragliche Pflichten mit dem Unterauftragsverarbeiter zu vereinbaren, falls diese Pflichten angemessene Datenschutzmaßnahmen gemäß der DSGVO enthalten, oder (b) die Standardvertragsklauseln mit dem Kunden zugunsten dieses Datenimporteurs abzuschließen.
- iv. Esri wird personenbezogene Daten nicht 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 den 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 anderen 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 von den geltenden Datenschutzgesetzen 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 Unter-Auftragsverarbeiter wie z. B. Microsoft Corporation, Amazon Web Services Inc., Salesforce.com Inc. und ihre verbundenen Unternehmen, Akamai Technologies, Inc. (einschließlich ihrer verbundenen 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 Beantwortung dieser Anfragen verantwortlich; Esri wird jedoch angemessen mit dem Kunden zusammenarbeiten, um derartige Anfragen zu klären. Dies gilt auch für Anfragen von natürlichen Personen, deren personenbezogene Daten zwecks Zugriff, Berichtigung, Widerspruch, Übertragbarkeit, Beschränkung, Löschung oder Export von Esri vorgehalten werden.
 - 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 vor Verlust, Missbrauch sowie unberechtigtem Zugriff, Offenlegung, Veränderung und Zerstörung zu schützen. 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 Nachtrags 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 anderen für den Kunden geltenden Datenschutzgesetzen erfolgt.

- 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. Alle Ausgaben im Zusammenhang mit diesem Unterabschnitt F sind vom Kunden zu tragen, sofern Esri nicht ein erheblicher Verstoß nachgewiesen wird.
- 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.

ZUM ZEUGNIS DESSEN bestätigen die Parteien ihre Zustimmung zum Vorangehenden durch ordnungsgemäße Ausfertigung dieses Anhangs durch ihre jeweils bevollmächtigten Vertreter. Der Anhang darf von keiner der Parteien geändert oder ergänzt werden, mit Ausnahme durch ein gesondertes und von beiden Parteien unterzeichnetes Schriftstück.

(Kunde)

unterzeichnet von: _____
Bevollmächtigter (Unterschrift)

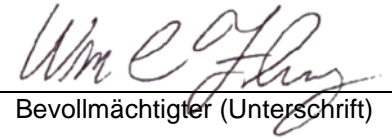
Name (Druckschrift): _____

Titel: _____

Datum: _____

Kundennummer: _____

ENVIRONMENTAL SYSTEMS
RESEARCH INSTITUTE, INC.
(Esri)

unterzeichnet von: 
Bevollmächtigter (Unterschrift)

Name (Druckschrift): William C. Fleming

Titel: Director, Contracts and Legal

NACHTRAG 1
STANDARDVERTRAGSKLAUSELN
Verantwortlicher an Auftragsverarbeiter

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)¹ bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.
- (b) Die Parteien:
- i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und
 - ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“),
- haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) einverstanden erklärt.
- (c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.
- (d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

- (a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.
- (b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

¹ Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG ([ABl. L 295 vom 21.11.2018, S. 39](#)), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

Klausel 3

Drittbegünstigte

- (a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:
- (i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7;
 - (ii) Klausel 8.1(b), 8.9(a), (c), (d) und (e);
 - (iii) Klausel 9(a), (c), (d) und (e);
 - (iv) Klausel 12(a), (d) und (f);
 - (v) Klausel 13;
 - (vi) Klausel 15.1(c), (d) und (e);
 - (vii) Klausel 16(e);
 - (viii) Klausel 18(a) und (b).
- (b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4

Auslegung

- (a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.
- (b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
- (c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6

Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7

Kopplungsklausel

- (a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und Anhang I.A unterzeichnet.
- (b) Nach Ausfüllen der Anlage und Unterzeichnung von Anhang I.A wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in Anhang I.A.
- (c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

8.1. Weisungen

- (a) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.
- (b) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann.

8.2 Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3 Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.4 Richtigkeit

Stellt der Datenimporteur fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Datenimporteur mit dem Datenexporteur zusammen, um die Daten zu löschen oder zu berichtigen.

8.5. Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

Die Daten werden vom Datenimporteur nur für die in Anhang I.B angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Datenimporteur nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e, den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14 Buchstabe a im Einklang stehen.

8.6 Sicherheit der Verarbeitung

- (a) Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen

Kontrolle des Datenexporteurs. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

- (b) Der Datenimporteur gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (c) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.
- (d) Unter Berücksichtigung der Art der Verarbeitung und der dem Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8.7 Sensible Daten

Soweit die Übermittlung personenbezogener Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Datenimporteur die in Anhang I.B beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8 Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union² ansässig sind (im Folgenden „Weiterübermittlung“), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran einverstanden erklärt oder falls

- (i) die Weiterübermittlung an ein Land erfolgt, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,
- (ii) der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung gewährleistet,
- (iii) die Weiterübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder
- (iv) die Weiterübermittlung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

² Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9 Dokumentation und Einhaltung der Klauseln

- (a) Der Datenimporteur bearbeitet Anfragen des Datenexporteurs, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.
- (b) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.
- (c) Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten Pflichten nachzuweisen; auf Verlangen des Datenexporteurs ermöglicht er diesem, die unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung zu prüfen, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.
- (d) Der Datenexporteur kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Datenimporteurs umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- (e) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben b und c genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 9

Einsatz von Unterauftragsverarbeitern

- (a) Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens dreißig (30) Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Datenexporteur damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Datenexporteur die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- (b) Beauftragung der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen.³ Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.
- (c) Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- (d) Der Datenimporteur haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Datenimporteur geschlossenen Vertrag nachkommt. Der Datenimporteur benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.
- (e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

³ Diese Anforderung ist gegebenenfalls vom Unterauftragsverarbeiter zu erfüllen, der diesen Klauseln gemäß Klausel 7 im Rahmen des betreffenden Moduls beiträgt.

Klausel 10

Rechte betroffener Personen

- (a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.
- (b) Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.
- (c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Datenimporteur die Weisungen des Datenexporteurs.

Klausel 11

Rechtsbehelf

- (a) Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

Der Datenimporteur erklärt sich damit einverstanden, dass betroffene Personen eine Beschwerde auch bei einer unabhängigen Streitbelegungsstelle⁴ einreichen können, ohne dass für die betroffene Person Kosten entstehen. Er unterrichtet die betroffenen Personen in der unter Buchstabe a beschriebenen Weise über einen solchen Rechtsbehelfsmechanismus sowie darüber, dass sie nicht verpflichtet sind, davon Gebrauch zu machen oder bei der Einlegung eines Rechtsbehelfs eine bestimmte Reihenfolge einzuhalten.
- (b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.
- (c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,
 - (i) eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,
 - (ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.
- (d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.
- (e) Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.
- (f) Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12

Haftung

- (a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.
- (b) Der Datenimporteur haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

⁴ Der Datenimporteur darf eine unabhängige Streitbeilegung über eine Schiedsstelle nur dann anbieten, wenn er in einem Land niedergelassen ist, das das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche ratifiziert hat.

- (c) Ungeachtet von Buchstabe b haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.
- (d) Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Buchstabe c für durch den Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs für den Schaden entspricht.
- (e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.
- (f) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe e haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.
- (g) Der Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

- (a) **Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:** Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:

Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen: Die Aufsichtsbehörde eines der Mitgliedstaaten, in denen die betroffenen Personen niedergelassen sind, deren personenbezogene Daten gemäß diesen Klauseln im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen übermittelt werden oder deren Verhalten beobachtet wird, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

- (b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

ABSCHNITT III — LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

- (a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass

Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

- (b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:
- (i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanaäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,
 - (ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien,⁵
 - (iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.
- (c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.
- (d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- (e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.
- (f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

⁵ Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. Dies betrifft insbesondere interne Aufzeichnungen oder sonstige Belege, die fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden, sofern diese Informationen rechtmäßig an Dritte weitergegeben werden können. Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden; den Parteien obliegt die sorgfältige Prüfung, ob alle diese Elemente ausreichend zuverlässig und repräsentativ sind, um die getroffene Schlussfolgerung zu bekräftigen. Insbesondere müssen die Parteien berücksichtigen, ob ihre praktische Erfahrung durch öffentlich verfügbare oder anderweitig zugängliche zuverlässige Informationen über das Vorhandensein oder Nicht-Vorhandensein von Ersuchen innerhalb desselben Wirtschaftszweigs und/oder über die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsgremien, erhärtet und nicht widerlegt wird.

Klausel 15

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

15.1 Benachrichtigung

- (a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,
 - (i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder
 - (ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.
- (b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.
- (c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).
- (d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- (e) Die Buchstaben a bis c gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2 Überprüfung der Rechtmäßigkeit und Datenminimierung

- (a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14 Buchstabe e.
- (b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.
- (c) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV — SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

- (a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- (b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.
- (c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - (i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,
 - (ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder
 - (iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt. In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.
- (d) Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.
- (e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Irland ist.

Klausel 18

Gerichtsstand und der Zuständigkeit

- (a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.
- (b) Die Parteien vereinbaren, dass dies die Gerichte von Irland sind.
- (c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.
- (d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANLAGE

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur(e):

1. **Name:** Wie in der Vereinbarung und diesem Nachtrag 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 Nachtrags durch jede Partei gilt als Unterzeichnung dieser Klauseln.

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Datenimporteure(e):

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

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

Name, Position und Kontaktdaten der Kontaktperson: Beauftragter für Informationssicherheit, 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 Nachtrags durch jede Partei gilt als Unterzeichnung dieser Klauseln.

Rolle (Verantwortlicher/Auftragsverarbeiter): Auftragsverarbeiter

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

Personen, über die Esri über 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

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben): Personenbezogene Daten, die Esri über die Online- und Abonnement- sowie Wartungsdienste vom (oder auf Anweisung) des Kunden oder der Endnutzer des Kunden 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 Kundendaten gemäß den Standards für sensible Daten, indem es die in Anhang 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 anderweitige Bereitstellung, Abgleich oder Kombination, Einschränkung, Löschung oder Vernichtung.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben): Betroffene Personen sind Personen, deren Daten an Esri über die Online- und Abonnement- sowie Wartungsdienste vom (oder auf Anweisung) des Kunden oder der Endnutzer des Kunden zur Verfügung gestellt werden.

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 aufbewahrt 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 technische Unterstützungsdienste mit einer Verarbeitung der gleichen Art und Dauer wie oben beschrieben.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

ANHANG II TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH 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 Dienste. Esri hat die folgenden, technischen Maßnahmen für die oben genannten ArcGIS Online-Dienste 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, verwaltet, gespeichert, zur Identifizierung des vorgesehenen Empfängers verlinkt 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 Public Key-Zertifizierungsbehörde und Infrastruktur 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, was es dem Kunden (Datenexporteur) erlaubt, personenbezogene Daten unter Aufsicht des Kunden (Datenexporteur) 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 kann, 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 Datenschutzerklärung (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 vordefinierten Nachtrag 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 Sicherheitspolitik des Unternehmens, 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 Nachtrag 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 Strafbüße) durch schriftliche Benachrichtigung an Esri kündigen.