Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Übersetzung

Abkommen über den digitalen Handel
zwischen den EFTA-Staaten und der Republik Singapur

Zur Änderung des Freihandelsabkommens
zwischen den EFTA-Staaten und der Republik Singapur

Abgeschlossen am 25. September 2025
Von der Bundesversammlung genehmigt am…
In Kraft getreten durch Notenaustausch am…

Präambel

Die Republik Island, das Fürstentum Liechtenstein, das Königreich Norwegen und die Schweizerische Eidgenossenschaft (nachfolgend als «EFTA-Staaten» bezeichnet) und
der Republik Singapur (nachfolgend als «Singapur» bezeichnet),
nachfolgend als «Vertragsparteien» bezeichnet,

in Anerkennung ihrer engen und langjährigen Beziehungen, deren Grundlage das am 26. Juni 2002 in Egilsstadir, Island, zwischen den EFTA-Staaten und Singapur abgeschlossene Freihandelsabkommen[1] (nachstehend als das «Freihandelsabkommen» oder in Anhang I und Anhang II als «dieses Abkommen» bezeichnet) bildet,

als Ausdruck ihrer gemeinsamen Vision für eine stärkere Integration und für die digitale Transformation ihrer Volkswirtschaften sowie ihrer Verpflichtung zur Vertiefung der Zusammenarbeit in neuen und aufkommenden Bereichen,

in Anerkennung der wirtschaftlichen Chancen und des erweiterten Zugangs zu Waren und Dienstleistungen, die mit der digitalen Wirtschaft einhergehen,

in Anerkennung der Bedeutung der digitalen Wirtschaft und der Tatsache, dass anhaltendes Wirtschaftswachstum von ihrer gemeinsamen Fähigkeit abhängt, technologische Innovationen zu nutzen, um bestehende Unternehmen zu verbessern und neue Produkte und Märkte zu schaffen,

in der Überzeugung, dass das folgende Abkommen über die digitale Wirtschaft die Wettbewerbsfähigkeit ihrer Unternehmen auf den Weltmärkten weiter steigern und zusätzliche Voraussetzungen schaffen wird, die für die Handels- und Investitionsbeziehungen zwischen den Vertragsparteien förderlich sind,

in Anerkennung der Rolle von Standards, insbesondere von offenen Standards, zur Erleichterung der Interoperabilität zwischen digitalen Systemen und zur Förderung höherwertiger Produkte und Dienstleistungen,

SR .....
1 SR **0.632.316.891.1**

im Wissen darum, wie wichtig es ist, sicherzustellen, dass alle Personen und Unternehmen jeder Grösse, einschliesslich kleiner und mittlerer Unternehmen (nachfolgend als «KMU» bezeichnet), an der digitalen Wirtschaft teilhaben, zu ihr beitragen und von ihr profitieren können,

in Anerkennung ihrer gegenseitigen Abhängigkeit in Fragen im Zusammenhang mit der digitalen Wirtschaft und – als führende Online-Wirtschaften – ihres gemeinsamen Interesses am Schutz kritischer Infrastrukturen und an der Gewährleistung eines sicheren, zuverlässigen Internets, das Innovation und die wirtschaftliche und soziale Entwicklung unterstützt,

entschlossen, ein vertrauenswürdiges, sicheres digitales Umfeld zu ermöglichen, das für den Konsumentenschutz und die Geschäftsinteressen förderlich ist,

in Bekräftigung des Rechts, zur Erreichung legitimer politischer Ziele im Bereich des digitalen Handels im Einklang mit dem folgenden Abkommen über die digitale Wirtschaft Regelungen zu erlassen,

in Bekräftigung ihres Bekenntnisses, das Ziel der nachhaltigen Entwicklung zu verfolgen, und in Anerkennung der Rolle des digitalen Handels zur Nutzung des Beitrags des internationalen Handels für die Förderung der nachhaltigen Entwicklung,

entschlossen, aufbauend auf ihren jeweiligen Rechten und Pflichten aus dem Abkommen von Marrakesch zur Errichtung der Welthandelsorganisation und den anderen in diesem Rahmen ausgehandelten Abkommen sowie auf ihrem Engagement innerhalb der Welthandelsorganisation das multilaterale Handelssystem zu fördern und weiter zu stärken und damit zur harmonischen Entwicklung und Ausweitung des Welthandels beizutragen,

haben zur Erreichung dieser Ziele folgendes Abkommen über die digitale Wirtschaft abgeschlossen:

Art. 1 Änderung des Freihandelsabkommens

In Übereinstimmung mit Artikel 69 (Änderungen) des Freihandelsabkommens vereinbaren die Vertragsparteien:

(a) im Anschluss an Kapitel III (Dienstleistungen) des Freihandelsabkommens ein neues Kapitel III^{bis} (Digitale Wirtschaft) gemäss Anhang I dieses Abkommens über die digitale Wirtschaft einzufügen; und

(b) in Anhang VIII (Finanzdienstleistungen) des Freihandelsabkommens im Anschluss an Artikel 5 einen neuen Artikel 5bis (Standort der Rechenanlagen für Finanzdienstleistungen) gemäss Anhang II dieses Abkommens über die digitale Wirtschaft einzufügen.

Art. 2 Informationsaustausch und Einbeziehung der Stakeholder

1. Jede Vertragspartei erstellt oder unterhält ihre eigene kostenlose, öffentlich zugängliche und regelmässig aktualisierte Website, auf der sie Informationen zu diesem

Abkommen über die digitale Wirtschaft bereitstellt. Soweit möglich sind die Informationen in englischer Sprache zur Verfügung zu stellen; sie können Folgendes umfassen:

(a) den Wortlaut dieses Abkommens über die digitale Wirtschaft;

(b) eine Zusammenfassung dieses Abkommens über die digitale Wirtschaft;

(c) Informationen für KMU, einschliesslich:

i) einer Beschreibung der Bestimmungen dieses Abkommens über die digitale Wirtschaft, die nach Einschätzung der betreffenden Vertragspartei für KMU von Bedeutung sind,

ii) zusätzlicher Informationen, die gegebenenfalls nützlich sind für KMU, die von den sich aus diesem Abkommen über die digitale Wirtschaft ergebenden Möglichkeiten profitieren möchten; und

(d) Links zu ähnlichen Websites über dieses Abkommen über die digitale Wirtschaft.

2. Die Vertragsparteien anerkennen, wie wichtig es ist, gegebenenfalls die Stakeholder einzubeziehen und einschlägige Initiativen und Plattformen innerhalb der sowie zwischen den Vertragsparteien zu fördern.

3. Die Vertragsparteien können gegebenenfalls interessierte Stakeholder wie Unternehmen, Nichtregierungsorganisationen und wissenschaftliche Sachverständige bei der Umsetzung und weiteren Modernisierung dieses Abkommens über die digitale Wirtschaft einbeziehen.

Art. 3 Inkrafttreten

1. Dieses Abkommen über die digitale Wirtschaft unterliegt der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Depositar des Freihandelsabkommens (nachfolgend als der «Depositar» bezeichnet) hinterlegt.

2. Für diejenigen Staaten, die ihre Ratifikations-, Annahme- oder Genehmigungsurkunde hinterlegt haben, tritt dieses Abkommen über die digitale Wirtschaft am ersten Tag des dritten Monats nach dem Zeitpunkt in Kraft, zu dem mindestens ein EFTA-Staat und Singapur ihre Ratifikations-, Annahme- oder Genehmigungsurkunde beim Depositar hinterlegt haben.

3. Für einen EFTA-Staat, der seine Ratifikations-, Annahme- oder Genehmigungsurkunde nach dem Zeitpunkt hinterlegt, zu dem mindestens ein EFTA-Staat und Singapur ihre Ratifikations-, Annahme- oder Genehmigungsurkunde beim Depositar hinterlegt haben, tritt dieses Abkommen über die digitale Wirtschaft am ersten Tag des dritten Monats nach Hinterlegung seiner Urkunde in Kraft.

Zu Urkund dessen haben die hierzu von ihrer jeweiligen Regierung gebührend bevollmächtigten Unterzeichner dieses Abkommen über die digitale Wirtschaft unterschrieben.

Geschehen zu Bern am 25. September 2025 in einer Urschrift in englischer Sprache, die beim Depositar hinterlegt wird. Der Depositar lässt allen Vertragsparteien beglaubigte Kopien zukommen.

Für
Island:

Für
die Republik Singapur:

Für
das Fürstentum Liechtenstein:

Für
das Königreich Norwegen:

Für
die Schweizerische Eidgenossenschaft:

Anhang I

Kapitel III[bis] Digitale Wirtschaft

Art. 36-A Begriffsbestimmungen

1. Für die Zwecke dieses Kapitels ist Artikel 22 anwendbar.
2. Für die Zwecke dieses Kapitels bedeutet:
   (a) «Rechenanlagen» Computerserver und Speichergeräte zur Bearbeitung oder Speicherung von Informationen für kommerzielle Zwecke, nicht jedoch Computerserver oder Speichergeräte von oder für den Zugang zu Finanzmarktinfrastrukturen;
   (b) «Kryptografie» die Grundsätze, Mittel oder Methoden zur Umwandlung von Daten, um ihren Inhalt geheim zu halten oder zu verbergen, unbemerkte Veränderungen daran zu vermeiden oder deren unerlaubte Nutzung zu verhindern;
   (c) «kryptografischer Algorithmus» ein festgelegtes Verfahren oder eine festgelegte Formel zur Umwandlung von Daten mithilfe der Kryptografie;
   (d) «elektronische Authentifizierung» den Vorgang oder die Durchführung der Überprüfung der Identität einer an einer elektronischen Kommunikation oder Transaktion beteiligten Partei oder den Vorgang und die Durchführung der Gewährleistung der Integrität einer elektronischen Kommunikation;
   (e) «elektronische Signatur» Daten in elektronischer Form, die einer elektronischen Datennachricht beigefügt oder mit ihr logisch verbunden werden und dazu genutzt werden können, um die unterzeichnende Person der Datennachricht zu identifizieren und ihre Genehmigung der in der betreffenden Datennachricht enthaltenen Informationen anzuzeigen[2];
   (f) «elektronische übertragbare Aufzeichnung» ein Dokument oder Instrument in elektronischer Form, das nach den Gesetzen oder sonstigen Vorschriften einer Vertragspartei sowohl funktional mit einer übertragbaren Aufzeichnung gleichwertig ist als auch Qualitätsanforderungen erfüllt wie diejenigen, die in Artikel 10 des UNCITRAL-Modellgesetzes zu elektronischen übertragbaren Aufzeichnungen (*Model Law on Electronic Transferable Records,* MLETR) von 2017 aufgeführt sind;
   (g) «elektronische Übermittlung» oder «elektronisch übermitteln» eine Übermittlung mithilfe elektromagnetischer Mittel, einschliesslich photonischer Mittel, z. B. über das Internet;

[2] Im Interesse grösserer Rechtssicherheit hindert nichts in dieser Bestimmung eine Vertragspartei daran, einer elektronischen Signatur grössere Rechtswirkung zu verleihen, sofern diese bestimmte Anforderungen erfüllt, etwa wenn sie die Angabe enthält, dass die elektronische Datennachricht nicht verändert wurde, oder wenn sie die Identität der unterzeichnenden Person überprüft.

(h) «Endnutzerin» bzw. «Endnutzer» eine Person, die bei einem Anbieter von Internetzugangsdiensten einen Internetzugangsdienst erwirbt oder abonniert;

(i) «Schlüssel» einen Parameter, der in Verbindung mit einem kryptografischen Algorithmus verwendet wird und dessen Funktionsweise so bestimmt, dass eine Person, die den Schlüssel kennt, den Vorgang reproduzieren oder umkehren kann, während eine Person ohne Kenntnis des Schlüssels dies nicht kann;

(j) «Metadaten» strukturelle oder beschreibende Informationen über Daten wie Inhalt, Format, Quelle, Rechte, Richtigkeit, Herkunft, Häufigkeit, Periodizität, Granularität, Herausgeber oder verantwortliche Partei, Kontaktdaten, Beschaffungsmethode und Kontext;

(k) «Personendaten» alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

(l) «Handelsverwaltungsdokumente» Formulare und Dokumente, die eine Vertragspartei ausstellt oder kontrolliert und die durch oder für einen Importeur oder Exporteur im Zusammenhang mit der Ein-, Aus- oder Durchfuhr von Waren ausgefüllt werden müssen;

(m) «Steuerabkommen» ein Abkommen zur Vermeidung der Doppelbesteuerung oder ein anderes internationales Steuerabkommen oder eine internationale Steuervereinbarung;

(n) «unerwünschte Werbenachrichten (Spam)» elektronische Nachrichten, die ohne Zustimmung der Empfängerin bzw. des Empfängers oder trotz der ausdrücklichen Ablehnung der Empfängerin bzw. des Empfängers zu Werbe- oder kommerziellen Zwecken an eine elektronische Adresse einer Person gesendet werden.

Art. 36-B Geltungsbereich

1. Dieses Kapitel gilt für Massnahmen einer Vertragspartei, die sich auf den elektronischen Handel auswirken.

2. Im Falle einer Unvereinbarkeit zwischen diesem Kapitel und Anhang VIII, hat bezüglich dieser Unvereinbarkeit Anhang VIII Vorrang.

3. Dieses Kapitel gilt nicht für:

(a) audiovisuelle Dienstleistungen[3];

(b) öffentliche Beschaffungen, vorbehaltlich von Artikel 36-E Absatz 1, Artikel 36-G Absatz 3 und Artikel 36-Z; oder

(c) Informationen, die von einer Vertragspartei oder in ihrem Namen gehalten oder bearbeitet werden, oder Massnahmen einer Vertragspartei im Zusam-

[3] Die Vertragsparteien kommen überein, dass dies auch den Rundfunk einschliesst, d. h. für die Zwecke dieses Abkommens die Übermittlung von Zeichen oder Signalen mittels beliebiger Technologien zum Empfang oder zur Wiedergabe von Ton- und Bildsignalen durch die gesamte oder einen Teil der Öffentlichkeit.

menhang mit diesen Informationen, einschliesslich Massnahmen im Zusammenhang mit ihrer Beschaffung, vorbehaltlich von Artikel 36-I.

Art. 36-C Zielsetzung

Die Vertragsparteien sind bestrebt:

(a) Rechtssicherheit und Vorhersehbarkeit für den elektronischen Handel zu gewährleisten;

(b) Hemmnisse für die Nutzung und Weiterentwicklung des digitalen Handels mit Waren und Dienstleistungen zu vermeiden;

(c) ein vertrauenswürdiges und sicheres Umfeld sowie Sicherheit für den digitalen Handel zu schaffen, unter anderem durch:

(i) den Schutz von Personendaten, und

(ii) den Schutz von Geschäftsgeheimnissen;

(d) die Zusammenarbeit zwischen den Vertragsparteien in Fragen von gemeinsamem Interesse, die die digitale Wirtschaft betreffen, auszuweiten;

(e) das Wachstum der Wirtschaftstätigkeit zwischen den Vertragsparteien zu fördern;

(f) zur Etablierung neuer, ehrgeiziger und transparenter Benchmarks beizutragen, die das Wachstum und die wirksame Regulierung der digitalen Wirtschaft fördern;

(g) auf den multilateralen und regionalen Verpflichtungen der Vertragsparteien zum digitalen Handel aufzubauen;

(h) stärkere Verbindungen zwischen Unternehmen der jeweiligen Vertragsparteien sowie zwischen ihren Forschungseinrichtungen zu erleichtern.

Art. 36-D Zölle[4]

1. Keine Vertragspartei erhebt Zölle auf elektronische Übermittlungen, einschliesslich auf elektronisch übertragene Inhalte.

2. Im Interesse grösserer Rechtssicherheit hindert Absatz 1 eine Vertragspartei nicht daran, inländische Steuern, Gebühren oder andere Abgaben auf elektronische Übermittlungen, einschliesslich auf elektronisch übertragene Inhalte zu erheben, sofern dies in einer Weise erfolgt, die mit diesem Abkommen vereinbar ist.

Art. 36-E Elektronische Authentifizierung

1. Sofern in ihren Gesetzen und sonstigen Vorschriften nichts anderes vorgesehen ist, darf eine Vertragspartei die Rechtswirkung, die Rechtsgültigkeit oder die Zulässigkeit einer elektronischen Signatur als Beweismittel in Gerichtsverfahren nicht allein mit der Begründung verweigern, dass sie in elektronischer Form vorliegt.

4 Die Vertragsparteien kommen überein, dass «Zölle» Einfuhr- und Ausfuhrzölle umfassen.

2. Keine Vertragspartei darf Massnahmen ergreifen oder aufrechterhalten, die:

(a) den an einer elektronischen Transaktion Beteiligten untersagen würden, gegenseitig die geeigneten elektronischen Authentifizierungsmethoden oder elektronischen Signaturen für ihre Transaktion festzulegen; oder

(b) verhindern würden, dass an einer elektronischen Transaktion beteiligte Parteien gegenüber den Justiz- und Verwaltungsbehörden nachweisen können, dass die Verwendung einer elektronischen Authentifizierung oder einer elektronischen Signatur bei dieser Transaktion den geltenden rechtlichen Anforderungen entspricht.

3. Ungeachtet von Absatz 2 kann eine Vertragspartei für eine bestimmte Kategorie von Transaktionen verlangen, dass die Authentifizierungsmethode oder die elektronische Signatur gemäss ihren Gesetzen und sonstigen Vorschriften bestimmte Leistungsstandards erfüllt oder von einer akkreditierten Behörde zertifiziert ist.

4. Eine Vertragspartei wendet die Absätze 1–3 in dem in ihren Gesetzen und sonstigen Vorschriften vorgesehenen Umfang auf elektronische Siegel, elektronische Zeitstempel oder Dienste für die Zustellung elektronischer Einschreiben an.

5. Die Vertragsparteien sind bestrebt, eine interoperable elektronische Authentifizierung zu verwenden.

Art. 36-F Papierloser Handel

1. Jede Vertragspartei macht elektronische Versionen aller Handelsverwaltungsdokumente öffentlich zugänglich, wenn möglich in englischer Sprache.[5]

2. Jede Vertragspartei anerkennt elektronische Versionen von Handelsverwaltungsdokumenten als rechtlich gleichwertig mit Papierdokumenten, ausser:

(a) es besteht eine gegenteilige innerstaatliche oder internationale rechtliche Anforderung; oder

(b) dies würde die Wirksamkeit der Handelsverwaltungsprozesse reduzieren.

3. Die Vertragsparteien sind bestrebt, einen zentralen Schalter einzurichten oder aufrechtzuerhalten, der Händlern die Einreichung der für die Einfuhr, Ausfuhr oder Durchfuhr von Waren erforderlichen Dokumente und Daten bei den beteiligten Behörden und Stellen an einer einzigen Stelle ermöglicht.

4. Die Vertragsparteien anerkennen, wie wichtig es ist, sofern angebracht in jeder Gerichtsbarkeit, den Austausch elektronischer Aufzeichnungen, die für Handelstätigkeiten zwischen ihren Unternehmen verwendet werden, zu erleichtern.

5. Die Vertragsparteien sind bestrebt, Datenaustauschsysteme zu entwickeln für den erleichterten Austausch von:

(a) Daten im Zusammenhang mit Handelsverwaltungsdokumenten zwischen den zuständigen Behörden jeder Vertragspartei; und

[5] Im Interesse grösserer Rechtssicherheit bedeutet elektronische Versionen von Handelsverwaltungsdokumenten entsprechende Dokumente in einem maschinenlesbaren Format.

(b) elektronischen Aufzeichnungen, die für Handelstätigkeiten zwischen ihren jeweiligen Unternehmen verwendet werden, sofern angebracht in jeder Gerichtsbarkeit.

6. Die Vertragsparteien anerkennen den Vorteil kompatibler und interoperabler Datenaustauschsysteme. Zu diesem Zweck sind die Vertragsparteien bestrebt, auf die Entwicklung und Einführung international anerkannter Standards für die Entwicklung und die Governance von Datenaustauschsystemen hinzuarbeiten.

7. Die Vertragsparteien sind bestrebt, bei neuen Initiativen, die die Nutzung und Einführung der in Absatz 5 genannten Datenaustauschsysteme fördern, stärken, unterstützen und erleichtern, zu kooperieren und zusammenzuarbeiten, namentlich durch:

(a) den Austausch von Informationen und Erfahrungen, einschliesslich in Bezug auf Best Practices im Bereich der Entwicklung und Governance von Datenaustauschsystemen; und

(b) die Zusammenarbeit bei Pilotprojekten zur Entwicklung und Governance von Datenaustauschsystemen.

8. Die Vertragsparteien arbeiten im Rahmen bestehender internationaler Vereinbarungen und Abkommen zusammen, um die Anerkennung elektronischer Versionen von Handelsverwaltungsdokumenten zu fördern.

9. Bei der Erarbeitung von Initiativen, die die Nutzung des papierlosen Handels vorsehen, ist jede Vertragspartei bestrebt, von internationalen Organisationen vereinbarte Methoden zu berücksichtigen.

Art. 36-G Innerstaatlicher Rahmen für elektronische Transaktionen

1. Die Vertragsparteien anerkennen die Bedeutung von Rahmenwerken für elektronische Transaktionen. Jede Vertragspartei ist bestrebt, einen Rechtsrahmen für elektronische Transaktionen einzuführen oder aufrechtzuerhalten, der mit den Grundsätzen folgender Abkommen im Einklang steht:

(a) UNCITRAL-Modellgesetz zum elektronischen Geschäftsverkehr (*Model Law on Electronic Commerce,* MLEC) von 1996;

(b) Übereinkommen der Vereinten Nationen über die Verwendung elektronischer Mitteilungen bei internationalen Verträgen, abgeschlossenen in New York am 23. November 2005; und

(c) UNCITRAL-Modellgesetz zu elektronischen übertragbare Aufzeichnungen von 2017.

2. Jede Vertragspartei ist bestrebt:

(a) jeglichen unnötigen Regulierungsaufwand für elektronische Transaktionen zu vermeiden; und

(b) die Mitwirkung interessierter Personen an der Entwicklung ihres Rechtsrahmens für elektronische Transaktionen zu erleichtern.

3. Sofern in ihren Gesetzen und sonstigen Vorschriften nichts anderes vorgesehen ist, darf eine Vertragspartei die Rechtswirkung, die Rechtsgültigkeit oder die Vollstreck-

barkeit eines elektronischen Vertrags nicht allein mit der Begründung verweigern, dass der Vertrag auf elektronischem Wege zustande gekommen ist.

Art. 36-H Grundsätze für den Zugang zum Internet und die Nutzung des Internets für den digitalen Handel

Vorbehaltlich ihrer innerstaatlichen Politiken, Gesetze und sonstigen Vorschriften anerkennen die Vertragsparteien die Vorteile davon, sicherzustellen, dass die Endnutzerinnen und Endnutzer auf ihrem Hoheitsgebiet die Möglichkeit haben:

(a) unter Vorbehalt eines angemessenen Netzmanagements auf über das Internet verfügbare Dienste und Anwendungen ihrer Wahl zuzugreifen, diese zu verbreiten und zu nutzen;[6]

(b) Endnutzergeräte ihrer Wahl mit dem Internet zu verbinden, vorausgesetzt, diese Geräte erfüllen die Anforderungen in dem Hoheitsgebiet, in dem sie genutzt werden, und schaden dem Netzwerk nicht; und

(c) Zugang zu Informationen über die Netzmanagementpraktiken ihres Anbieters von Internetzugangsdiensten zu haben.

Art. 36-I Offene staatliche Daten (Open Government Data)

1. Dieser Artikel gilt für Massnahmen einer Vertragspartei betreffend Daten im Besitz des Staates, deren Offenlegung gemäss den Gesetzen und sonstigen Vorschriften dieses Staates nicht eingeschränkt ist und die eine Vertragspartei für den öffentlichen Zugang und die öffentliche Nutzung digital zur Verfügung stellt (nachfolgend als «staatliche Daten» bezeichnet).

2. Die Vertragsparteien anerkennen den Vorteil davon, staatliche Daten im Einklang mit den Absätzen 3–5 auf digitalem Weg für den öffentlichen Zugang und die öffentliche Nutzung zur Verfügung zu stellen. Die Vertragsparteien sind bestrebt, staatliche Daten kostenlos oder zu vertretbaren Kosten allgemein zur Verfügung zu stellen.

3. Die Vertragsparteien anerkennen, dass die Erleichterung des öffentlichen Zugangs zu und der öffentlichen Nutzung von staatlichen Daten die wirtschaftliche und soziale Entwicklung, die Wettbewerbsfähigkeit und die Innovation fördert. Zu diesem Zweck werden die Vertragsparteien aufgefordert, den Erfassungsbereich dieser Daten zu erweitern, etwa durch die Einbeziehung und die Konsultation interessierter Stakeholder.

4. Soweit sich eine Vertragspartei dafür entscheidet, staatliche Daten auf digitalem Weg für den öffentlichen Zugang und die öffentliche Nutzung zur Verfügung zu stellen, ist sie soweit durchführbar bestrebt, sicherzustellen, dass diese Daten:

(a) in einem maschinenlesbaren, offenen Format bereitgestellt werden;

(b) durchsuchbar und abrufbar sind;

(c) gegebenenfalls zeitnah aktualisiert werden; und

6 Die Vertragsparteien anerkennen, dass ein Anbieter von Internetzugangsdiensten, der seinen Abonnentinnen und Abonnenten bestimmte Inhalte auf Exklusivbasis anbietet, nicht gegen diesen Grundsatz verstossen würde.

(d) begleitet werden von Metadaten in gängigen Formaten, die es den Nutzerinnen und Nutzern ermöglichen, die Daten zu verstehen und zu nutzen.

5. Soweit sich eine Vertragspartei dafür entscheidet, staatliche Daten mit expliziter Quellenangabe auf digitalem Weg für den öffentlichen Zugang und die öffentliche Nutzung zur Verfügung zu stellen, ist sie bestrebt, dies nicht an Bedingungen[7] zu knüpfen, die die Nutzerinnen und Nutzer solcher Daten in unangemessener Weise daran hindern oder dabei einschränken:

(a) die Daten zu vervielfältigen, weiterzugeben oder erneut zu veröffentlichen;

(b) die Daten zusammenzufassen; oder

(c) die Daten zu kommerziellen oder nichtkommerziellen Zwecken, unter anderem bei der Herstellung eines neuen Produkts oder einer neuen Dienstleistung, zu nutzen.

6. Die Vertragsparteien sind bestrebt, unter anderem durch den Austausch von Informationen und Erfahrungen in Bezug auf Praktiken und Politiken in Angelegenheiten kooperieren, die es erlauben, im Hinblick auf die Verbesserung und Schaffung von Geschäfts- und Forschungsmöglichkeiten insbesondere für kleine und mittlere Unternehmen (nachfolgend als «KMU» bezeichnet) den öffentlichen Zugang zu und die öffentliche Nutzung von staatlichen Daten zu erleichtern und zu erweitern.

Art. 36-J Online-Konsumentenschutz

1. Die Vertragsparteien anerkennen die Bedeutung transparenter und wirksamer Massnahmen zur Stärkung des Vertrauens der Konsumentinnen und Konsumenten in Bezug auf den digitalen Handel. Jede Vertragspartei führt Massnahmen ein oder erhält diese aufrecht, mit denen irreführende, missbräuchliche und betrügerische Geschäftstätigkeiten, die den am digitalen Handel beteiligten[8] Konsumentinnen und Konsumenten Schaden zufügen oder zufügen könnten, verboten werden.

2. Als irreführende, missbräuchliche und betrügerische Geschäftstätigkeiten gelten:

(a) wesentliche Falschdarstellungen[9], einschliesslich impliziter sachlicher Falschdarstellungen oder falscher Behauptungen in Bezug auf Aspekte wie Qualität, Preis, Zwecktauglichkeit, Menge oder Ursprung der Waren oder Dienstleistungen;

(b) Werbung für die Lieferung von Waren oder zur Erbringung von Dienstleistungen, ohne dass die Absicht oder angemessene Möglichkeiten zur Lieferung oder Erbringung bestehen;

7 Im Interesse grösserer Rechtssicherheit hindert nichts in diesem Absatz eine Vertragspartei daran, die Nutzerinnen und Nutzer solcher Daten zur Angabe der Originalquelle zu verpflichten.

8 Der Begriff «beteiligt» umfasst auch die Phase des digitalen Handels, die einer Transaktion vorangeht.

9 Für die Zwecke dieses Artikels bezeichnet der Begriff «wesentliche Falschdarstellungen» nicht-wahrheitsgetreue Darstellungen, die das Verhalten oder die Entscheidung der Konsumentinnen und Konsumenten hinsichtlich der Nutzung oder des Kaufs einer Ware oder Dienstleistung beeinflussen könnten.

(c) das Versäumnis, den Konsumentinnen und Konsumenten Waren zu liefern oder für sie Dienstleistungen zu erbringen, nachdem ihnen diese in Rechnung gestellt wurden, es sei denn, dies ist aus triftigen Gründen gerechtfertigt; oder

(d) der Vorgang, den Konsumentinnen und Konsumenten Kosten für nicht angeforderte Dienstleistungen oder Waren in Rechnung zu stellen.

3. Zum Schutz der am digitalen Handel beteiligten Konsumentinnen und Konsumenten führt jede Vertragspartei Massnahmen ein oder erhält diese aufrecht, die gewährleisten sollen, dass:

(a) Anbieter von Waren und Dienstleistungen fair und ehrlich mit den Konsumentinnen und Konsumenten umgehen;

(b) Anbieter vollständige, korrekte und transparente Informationen über die Waren und Dienstleistungen bereitstellen, einschliesslich allfälliger Geschäftsbedingungen; und

(c) die Waren und gegebenenfalls die Dienstleistungen bei normaler oder vernünftigerweise vorhersehbarer Verwendung sicher sind.

4. Die Vertragsparteien anerkennen, wie wichtig es ist, den am digitalen Handel beteiligten Konsumentinnen und Konsumenten ein Konsumentenschutzniveau zu gewähren, das nicht unter demjenigen liegt, das den an anderen Formen des Handels beteiligten Konsumentinnen und Konsumenten gewährt wird.

5. Die Vertragsparteien anerkennen die Bedeutung der Zusammenarbeit zwischen ihren jeweiligen Konsumentenschutzbehörden oder anderen einschlägigen Stellen; dies schliesst den Austausch von Informationen und Erfahrungen ein sowie die Zusammenarbeit in geeigneten Fällen von gemeinsamem Interesse, die die Verletzung von Konsumentenrechten im digitalen Handel betreffen, und mit der der Konsumentenschutz im Online-Handel verbessert werden soll, sofern dies im gegenseitigen Einvernehmen vereinbart wird.

6. Die Vertragsparteien fördern den Zugang zu Mechanismen für die Durchsetzung von Konsumentenrechten sowie für den Rechtsschutz und steigern die Bekanntheit solcher Mechanismen, einschliesslich bei Konsumentinnen und Konsumenten, die grenzüberschreitende Transaktionen tätigen.

Art. 36-K Unerwünschte Werbenachrichten (Spam)

1. Jede Vertragspartei führt Massnahmen ein oder erhält diese aufrecht, um die Nutzerinnen und Nutzer wirksam vor unerwünschten Werbenachrichten zu schützen. Diese Massnahmen:

(a) verpflichten die Versenderinnen und Versender von unerwünschten Werbenachrichten, den Empfängerinnen und Empfängern eine einfache Möglichkeit zu bieten, um den fortlaufenden Erhalt solcher Nachrichten zu beenden; und

(b) erfordern, von den Empfängerinnen und Empfängern gemäss den innerstaatlichen Gesetzen und sonstigen Vorschriften der betreffenden Vertragspartei die Zustimmung zum Erhalt von Werbenachrichten zu verlangen.

2. Jede Vertragspartei ist bestrebt, sicherzustellen, dass unerwünschte Werbenachrichten klar als solche erkennbar sind, eindeutig offenlegen, in wessen Namen sie versendet wurden, und, soweit in ihren Gesetzen und sonstigen Vorschriften vorgesehen, alle erforderlichen Informationen enthalten, damit die Empfängerinnen und Empfänger jederzeit und kostenlos ihre Einstellung beantragen können.

3. Jede Vertragspartei sieht Rekursmöglichkeiten gegen die Versenderinnen und Versender unerwünschter Werbenachrichten vor, die sich nicht an die gemäss den Absätzen 1 und 2 eingeführten oder aufrechterhaltenen Massnahmen halten.

4. Die Vertragsparteien arbeiten in geeigneten Fällen von gemeinsamem Interesse in Bezug auf die Regulierung unerwünschter Werbenachrichten zusammen.

Art. 36-L Schutz von Personendaten

1. Die Vertragsparteien anerkennen, dass Einzelpersonen ein Recht auf Privatsphäre und den Schutz von Personendaten haben und dass hohe, durchsetzbare Standards in dieser Hinsicht zum Vertrauen in die digitale Wirtschaft und zur Entwicklung des Handels beitragen.

2. Zu diesem Zweck führt jede Vertragspartei einen Rechtsrahmen ein, der den wirksamen Schutz von Personendaten im digitalen Handel vorsieht, oder erhält einen solchen aufrecht.[10]

3. Nichts in diesem Abkommen hindert eine Vertragspartei daran, im Einklang mit ihrem Rechtsrahmen gemäss Absatz 2 von ihr als geeignet erachtete Massnahmen einzuführen oder aufrechtzuerhalten, einschliesslich mittels Erlass und Anwendung von Vorschriften für die grenzüberschreitende Übermittlung von Personendaten, sofern die Gesetze und sonstigen Vorschriften der betreffenden Vertragspartei Instrumente vorsehen, die Übermittlungen unter allgemeingültigen Bedingungen zum Schutz der übermittelten Daten ermöglichen.

4. Bei der Schaffung ihres Rechtsrahmen zum Schutz von Personendaten sollte jede Vertragspartei die von einschlägigen internationalen Gremien oder Organisationen entwickelten Grundsätze und Leitlinien berücksichtigen.

5. Jede Vertragspartei stellt sicher, dass ihr Rechtsrahmen gemäss Absatz 2 einen nicht-diskriminierenden Schutz von Personendaten für natürliche Personen vorsieht.

6. Jede Vertragspartei veröffentlicht im Zusammenhang mit dem Schutz von Personendaten Informationen über die Rechte, die sie natürlichen Personen im digitalen Handel gewährt, einschliesslich Leitlinien dazu, wie:

(a) natürliche Personen Rechtsmittel einlegen können; und

(b) wie Unternehmen die rechtlichen Anforderungen erfüllen können.

[10] Im Interesse grösserer Rechtssicherheit kann eine Vertragspartei der Pflicht gemäss Abs. 2 nachkommen, indem sie Massnahmen oder eine Kombination mehrerer Massnahmen einführt oder aufrechterhält, etwa umfassende Gesetze zum Schutz der Privatsphäre, von persönlichen Informationen und Personendaten, sektorspezifische Gesetze zum Schutz der Privatsphäre oder andere Gesetze, die sich mit der Verletzungen der Privatsphäre befassen.

7. Jede Vertragspartei ermutigt Unternehmen in ihrem Hoheitsgebiet, ihre Politiken und Verfahren zum Schutz von persönlichen Informationen zu veröffentlichen, insbesondere in Internet.

8. In Anerkennung der Tatsache, dass die Vertragsparteien beim Schutz von Personendaten unterschiedliche rechtliche Ansätze verfolgen können, regt jede Vertragspartei die Entwicklung von Mechanismen zur Förderung der Kompatibilität zwischen diesen verschiedenen Regelungen an. Diese Mechanismen können die autonom oder durch gegenseitige Vereinbarung erfolgte Anerkennung regulatorischer Ergebnisse oder breiter gefasste internationale Rechtsrahmen umfassen. Zu diesem Zweck sind die Vertragsparteien bestrebt, Informationen über die in ihren jeweiligen Gerichtsbarkeiten zur Anwendung kommenden Mechanismen auszutauschen.

Art. 36-M Grenzüberschreitender Datenfluss

1. Die Vertragsparteien verpflichten sich, die grenzüberschreitende Übermittlung von Daten auf elektronischem Wege sicherzustellen, wenn dies der Abwicklung von Geschäften unter diesem Abkommen dient.

2. Zu diesem Zweck darf eine Vertragspartei keine Massnahmen einführen oder aufrechterhalten, die die grenzüberschreitende Datenübermittlung nach Absatz 1 verbieten oder beschränken, indem sie:

(a) die Nutzung von Rechenanlagen oder Netzelementen im Hoheitsgebiet der Vertragspartei für die Datenbearbeitung vorschreibt, auch durch die Vorgabe der Nutzung von Rechenanlagen oder Netzelementen, die im Hoheitsgebiet der Vertragspartei zertifiziert oder zugelassen sind;

(b) die Lokalisierung von Daten im Hoheitsgebiet der Vertragspartei zur Speicherung oder Bearbeitung verlangt;

(c) die Speicherung oder Bearbeitung von Daten im Hoheitsgebiet einer anderen Vertragspartei verbietet;

(d) die grenzüberschreitende Übermittlung von Daten von der Nutzung von Rechenanlagen oder Netzelementen im Hoheitsgebiet der Vertragspartei oder von Lokalisierungsanforderungen im Hoheitsgebiet der Vertragspartei abhängig macht; oder

(e) die Datenübermittlung in das Hoheitsgebiet der Vertragspartei verbietet.[11]

3. Die Vertragsparteien überprüfen die Umsetzung dieser Bestimmung und bewerten ihr Funktionieren innerhalb von drei Jahren nach dem Inkrafttreten des am 25. September 2025 in Bern, Schweiz, abgeschlossenen Abkommens über die digitale Wirtschaft zwischen den EFTA-Staaten und Singapur. Eine Vertragspartei kann den anderen Vertragsparteien jederzeit vorschlagen, die Liste der in Absatz 2 aufgeführten Beschränkungen zu überprüfen, auch wenn sie selbst oder eine andere Vertragspartei

[11] Im Interesse grösserer Rechtssicherheit hindern die Anforderungen nach den Buchstaben a–d eine Vertragspartei nicht daran, die Speicherung von Informationen zur Rechnungslegung und zur Buchführung in ihrem Hoheitsgebiet zu verlangen, solange der grenzüberschreitende Datenfluss erlaubt ist.

vereinbart hat, in einem künftigen bilateralen oder multilateralen Abkommen keine anderen Arten von Massnahmen einzuführen oder aufrechtzuerhalten, die über die in Absatz 2 aufgeführten Massnahmen hinausgehen. Ein solches Ersuchen wird wohlwollend geprüft.

4. Nichts in diesem Artikel hindert eine Vertragspartei daran, zur Erreichung eines legitimen Politikziels[12] eine Massnahme einzuführen oder aufrechtzuerhalten, die mit Absatz 2 nicht vereinbar ist, sofern die betreffende Massnahme:

(a) nicht so angewendet wird, dass sie zu einer willkürlichen oder ungerechtfertigten Diskriminierung oder einer versteckten Handelsbeschränkung führt; und

(b) keine Beschränkungen für die Übermittlung von Informationen über das zur Umsetzung des Ziels erforderliche Mass hinaus vorschreibt.[13]

5. Dieser Artikel findet keine Anwendung auf «Finanzdienstleistungserbringer» gemäss der Begriffsbestimmung in Anhang VIII Artikel 1 Absatz II.

Art. 36-N Elektronische Bezahlmöglichkeiten

1. Die Vertragsparteien anerkennen die zentrale Rolle von elektronischen Bezahlmöglichkeiten für den digitalen Handel sowie das rasche Wachstum von elektronischen Zahlungen, einschliesslich der von Nichtbanken, Nicht-Finanzinstituten sowie von Unternehmen im Bereich der Finanztechnologie («FinTech») angebotenen Möglichkeiten. Die Vertragsparteien kommen überein, die Entwicklung effizienter, zuverlässiger und sicherer grenzüberschreitender elektronischer Bezahlmöglichkeiten zu unterstützen, indem sie die Einführung und Verwendung international akzeptierter Standards fördern, die Interoperabilität und Vernetzung von Zahlungsinfrastrukturen unterstützen und nützliche Innovationen sowie den Wettbewerb im Ökosystem des Zahlungsverkehrs anregen.

2. Jede Vertragspartei ist bestrebt:

(a) Regelungen zu elektronischen Bezahlmöglichkeiten öffentlich zugänglich zu machen, einschliesslich solche, die behördliche Genehmigungen, Zulassungsanforderungen, Verfahren und technische Standards betreffen;

(b) die Einführung internationaler Standards für elektronische Zahlungsverkehrsdaten zu fördern, die eine mehr Interoperabilität zwischen elektronischen Zahlungssystemen ermöglichen;

12 Für die Zwecke dieses Artikels wird der Begriff «legitimes Politikziel» objektiv ausgelegt und ermöglicht die Verfolgung von Zielen wie dem Schutz der öffentlichen Sicherheit, der öffentlichen Sittlichkeit oder des Lebens oder der Gesundheit von Menschen, Tieren oder Pflanzen oder der Aufrechterhaltung der öffentlichen Ordnung oder anderer Ziele von öffentlichem Interesse, wobei der Weiterentwicklung digitaler Technologien und den damit verbundenen Herausforderungen Rechnung getragen wird.

13 Im Interesse grösserer Rechtssicherheit sei darauf hingewiesen, dass diese Bestimmung die Auslegung anderer in diesem Abkommen vorgesehener Ausnahmen und ihre Anwendung auf diesen Artikel oder das Recht einer Vertragspartei, sich auf eine dieser Ausnahmen zu berufen, nicht berührt.

(c) Innovation und Wettbewerb unter gleichen Rahmenbedingungen sowie die zeitnahe Einführung neuer elektronischer Finanzierungs- und Zahlungsprodukte sowie -dienstleistungen zu erleichtern, indem beispielsweise regulatorische «Sandboxes» für die Branche eingeführt werden; und

(d) für Handels- und Finanztransaktionen die Einführung von Zahlungsinstrumenten oder -systemen zu fördern oder zu erleichtern, die sich auf die Technik verteilter elektronischer Register (Distributed-Ledger-Technologie, DLT) stützen, einschliesslich der Nutzung von *Smart Contracts* zur Effizienzsteigerung.

3. Die Vertragsparteien anerkennen, wie wichtig es ist, durch ihre jeweiligen Gesetze und sonstigen Vorschriften die Zuverlässigkeit, Effizienz, Vertrauenswürdigkeit und Sicherheit elektronischer Zahlungssysteme zu gewährleisten.

Art. 36-O Elektronische Rechnungsstellung

1. Die Vertragsparteien anerkennen die Bedeutung der elektronischen Rechnungsstellung zur Verbesserung der Effizienz, Genauigkeit und Zuverlässigkeit von Handelstransaktionen. Jede Vertragspartei anerkennt darüber hinaus die Vorteile, die sich daraus ergeben, wenn sichergestellt wird, dass die für die elektronische Rechnungsstellung in ihrem Hoheitsgebiet genutzten Systeme mit den Systemen, die für die elektronische Rechnungsstellung im Hoheitsgebiet einer anderen Vertragspartei verwendet werden, interoperabel sind.

2. Jede Vertragspartei ist bestrebt, sicherzustellen, dass die Umsetzung von Massnahmen im Zusammenhang mit der elektronischen Rechnungsstellung in ihrem Hoheitsgebiet für die grenzüberschreitende Interoperabilität zwischen den Rahmenbedingungen für die elektronische Rechnungsstellung der Vertragsparteien förderlich ist. Zu diesem Zweck berücksichtigen die Vertragsparteien internationale Rahmenwerke.

3. Die Vertragsparteien anerkennen die wirtschaftliche Bedeutung, die der Förderung der weltweiten Einführung interoperabler Systeme für die elektronische Rechnungsstellung zukommt. Zu diesem Zweck sind die Vertragsparteien bestrebt, sich gegebenenfalls über Best Practices im Zusammenhang mit der elektronischen Rechnungsstellung auszutauschen.

4. Die Vertragsparteien anerkennen die Vorteile von Initiativen, die die Einführung der elektronischen Rechnungsstellung durch Unternehmen fördern, anregen, unterstützen oder erleichtern. Zu diesem Zweck sind die Vertragsparteien bestrebt:

(a) Informationen und Erfahrungen einschliesslich Best Practices im Bereich der elektronischen Rechnungsstellung auszutauschen;

(b) das Vorhandensein von zugrundeliegenden Strategien, Infrastrukturen und Verfahren, die die elektronische Rechnungsstellung unterstützen, zu fördern; und

(c) das Bewusstsein für die elektronische Rechnungsstellung zu schaffen und die entsprechenden Kapazitäten aufzubauen.

Art. 36-P Quellcode[14]

1. Keine Vertragspartei verlangt die Weitergabe von oder den Zugriff auf Quellcodes von Software oder Teilen davon, die einer natürlichen oder juristischen Person einer anderen Vertragspartei gehören, als Bedingung für die Einfuhr, den Vertrieb, den Verkauf oder die Nutzung solcher Software oder von Produkten, die solche Software enthalten, in ihr bzw. in ihrem Hoheitsgebiet.

2. Absatz 1 findet keine Anwendung auf:

(a) Vorgaben eines Gerichts, einer Regulierungsbehörde oder einer anderen für eine Ermittlung, eine Inspektion, eine Überprüfung, ein Strafverfolgungs- oder ein Gerichtsverfahren zuständigen Stelle sowie auf die Überwachung der Einhaltung von Verhaltenskodizes und anderen Standards, vorbehaltlich des Schutzes vor unbefugter Weitergabe;

(b) die Verhängung, Einführung oder Durchsetzung einer Abhilfemassnahme, die in Übereinstimmung mit den Gesetzen und sonstigen Vorschriften einer Vertragspartei infolge einer Ermittlung, Inspektion, Überprüfung, einer Strafverfolgungsmassnahme oder eines Gerichtsverfahrens gewährt wurde;

(c) Vorgaben von zuständigen Behörden, mit denen die Konformität von Waren und Dienstleistungen mit Rechtsvorschriften im Zusammenhang mit der Marktüberwachung überprüft wird; oder

(d) die freiwillige Weitergabe von oder die Gewährung des Zugriffs auf Quellcodes auf kommerzieller Basis durch eine natürliche oder juristische Person einer Vertragspartei oder im Rahmen von Open-Source-Lizenzen.

Art. 36-Q Kryptografie verwendende Informations- und Kommunikationstechnologieprodukte

1. Für die Zwecke dieses Artikels bedeutet «Informations- und Kommunikationstechnologieprodukt (IKT-Podukt)» jegliche Hardware oder Software, die für die Informationsbearbeitung oder die Kommunikation mithilfe elektronischer Mittel, einschliesslich der Speicherung, Übermittlung und Anzeige, oder für die elektronische Bearbeitung zur Bestimmung oder Aufzeichnung physikalischer Phänomene oder zur Überprüfung physikalischer Prozesse konzipiert wurden, nicht jedoch Instrumente zur Erbringung einer Finanzdienstleistung oder Vermögenswerte, einschliesslich Währungen.

2. Dieser Artikel findet Anwendung IKT-Produkte, die Kryptografie verwenden.

3. In Bezug auf Produkte, die Kryptografie verwenden und für kommerzielle Anwendungen bestimmt sind, darf keine Vertragspartei technische Vorschriften oder Konformitätsbewertungsverfahren vorschreiben oder aufrechterhalten, die den Hersteller oder Lieferanten des Produkts als Voraussetzung für die Herstellung, den Verkauf, den Vertrieb, die Einfuhr oder die Verwendung des Produkts verpflichten:

14 Im Interesse grösserer Rechtssicherheit vereinbaren die Vertragsparteien, dass dieser Artikel eine Vertragspartei nicht daran hindert, für Patentanmeldungen und Patenterteilungsverfahren die Offenlegung des Quellcodes zu verlangen.

(a) eine bestimmte Technologie, ein bestimmtes Produktionsverfahren oder sonstige Informationen, zum Beispiel einen privaten Schlüssel oder andere geheime Parameter, die Spezifikation eines Algorithmus oder andere Designdetails, die Eigentum des Herstellers oder Lieferanten sind und sich auf die durch das Produkt verwendete Kryptografie beziehen, an die Vertragspartei oder eine Person im Hoheitsgebiet der Vertragspartei weiterzugeben oder ihr Zugriff darauf zu verschaffen;

(b) sich mit einer Person in ihrem Hoheitsgebiet zusammenzuschliessen; oder

(c) einen bestimmten kryptografischen Algorithmus zu verwenden oder zu integrieren;

es sei denn, die Herstellung, der Verkauf, der Vertrieb, die Einfuhr oder die Verwendung des Produkts erfolgt durch oder für die Vertragspartei.

4. Absatz 2 findet keine Anwendung auf:

(a) Vorgaben, die eine Vertragspartei in Bezug auf den Zugriff auf Netzwerke einführt oder aufrechterhält, einschliesslich auf Benutzergeräte, die sich im Besitz oder unter der Kontrolle der Regierung dieser Vertragspartei befinden, darunter auch diejenigen der Zentralbanken;

(b) Massnahmen, die eine Vertragspartei aufgrund von Aufsichts-, Untersuchungs- oder Überprüfungsbefugnissen im Zusammenhang mit Finanzinstituten oder -märkten ergreift; oder

(c) Vorgaben einer Regulierungs- oder einer Justizbehörde einer Vertragspartei in Bezug auf Informationen, auf die Absatz 2 Anwendung findet, im Zusammenhang mit einer Ermittlung, Inspektion, Überprüfung, eine Strafverfolgungsmassnahme oder für ein Gerichtsverfahren, vorbehaltlich des Schutzes vor unbefugter Weitergabe.

5. Im Interesse grösserer Rechtssicherheit ist dieser Artikel nicht so auszulegen, dass er die Strafverfolgungsbehörden einer Vertragspartei daran hindert, von Dienstleistungsanbietern, die eine von ihnen selbst kontrollierte Verschlüsselung verwenden, zu verlangen, dass sie in Übereinstimmung mit den rechtlichen Verfahren dieser Vertragspartei verschlüsselte und unverschlüsselte Kommunikation bereitstellen.

6. Im Interesse grösserer Rechtssicherheit lässt dieser Artikel die Rechte und Pflichten einer Vertragspartei nach Artikel 36-P unberührt.

Art. 36-R Cybersicherheit

1. Die Vertragsparteien haben eine gemeinsame Vision im Hinblick auf die Förderung eines sicheren digitalen Handels zur Erreichung weltweiten Wohlstands und anerkennen, dass Bedrohungen der Cybersicherheit das Vertrauen in den digitalen Handel untergraben. Entsprechend anerkennen die Vertragsparteien, wie wichtig es ist:

(a) die Kapazitäten ihrer jeweiligen, für die Reaktion auf Cybersicherheitsvorfälle zuständigen nationalen Einrichtungen auszubauen und dabei der sich stetig wandelnden Natur der Cyberbedrohungen Rechnung zu tragen;

(b) Mechanismen für die Zusammenarbeit zur Früherkennung, Ermittlung und Eindämmung böswilliger Eingriffe oder der Verbreitung schädlicher Programmcodes, die elektronische Netzwerke beeinträchtigen, einzurichten oder entsprechende bestehende Mechanismen zu stärken und diese zur raschen Bewältigung von Cybersicherheitsvorfällen zu nutzen;

(c) einen Dialog über Fragen der Cybersicherheit, einschliesslich des Austauschs von Informationen und Erfahrungen zur Sensibilisierung sowie über Best Practices aufrechtzuerhalten;

(d) eine gegenseitige Anerkennung eines grundlegenden Sicherheitsstandards für Verbrauchergeräte des Internets der Dinge zu einzurichten, um das allgemeine Niveau der Cyberhygiene zu erhöhen und den Cyberraum im Inland besser zu schützen; und

(e) die Personalentwicklung im Bereich der Cybersicherheit voranzutreiben, einschliesslich durch mögliche Aus- und Weiterbildungsinitiativen.

2. Angesichts der sich stetig wandelnden Natur der Cyberbedrohungen anerkennen die Vertragsparteien, dass risikobasierte Ansätze zur Bekämpfung solcher Bedrohungen wirksamer sein können als regelbasierte Ansätze. Die Vertragsparteien betonen daher die Vorteile der Einbeziehung von Sicherheitsaspekten in der Entwicklungsphase und sind bestrebt, risikobasierte Ansätze zu verwenden, die sich auf technische, objektive und interoperable Standards und Best Practices im Bereich Risikomanagement stützen, um Cybersicherheitsrisiken zu erkennen, sich davor zu schützen sowie um Cybersicherheitsvorfälle zu erkennen, darauf zu reagieren und sich davon zu erholen, und die Unternehmen in ihrem Hoheitsgebiet zur Nutzung solcher risikobasierter Ansätze zu ermutigen.

Art. 36-S Zusammenarbeit und Überprüfung

1. Die Vertragsparteien können zusätzlich zu den in diesem Kapitel festgelegten Bestimmungen zur themenspezifischen Zusammenarbeit in jeder anderen Angelegenheit von gemeinsamem Interesse im Zusammenhang mit dem digitalen Handel kooperieren, unter anderem bei folgenden Themen:

(a) Haftung von Anbietern von Vermittlungsdiensten in Bezug auf die Übermittlung und Speicherung von Informationen;

(b) Interoperabilität von Infrastrukturen wie die sichere elektronische Authentifizierung und sichere elektronische Bezahlmöglichkeiten; und

(c) Schutz von Personendaten.

2. Die Vertragsparteien überprüfen dieses Kapitel regelmässig im Gemischten Ausschuss hinsichtlich neuer Entwicklungen im Bereich des digitalen Handels.

Art. 36-T Zusammenarbeit im Bereich der Wettbewerbspolitik

1. In Anerkennung der Tatsache, dass die Vertragsparteien vom Austausch ihrer Erfahrungen mit der Durchsetzung des Wettbewerbsrechts sowie der Entwicklung und Einführung einer Wettbewerbspolitik zur Bewältigung der Herausforderungen im Zu-

sammenhang mit der digitalen Wirtschaft profitieren können, erwägen sie vorbehaltlich der verfügbaren Ressourcen auf technischer Ebene zusammenzuarbeiten, namentlich durch:

(a) den Austausch von Informationen und Erfahrungen im Zusammenhang mit die Entwicklung einer Wettbewerbspolitik für digitale Märkte;

(b) den Austausch von Best Practices zur Durchsetzung des Wettbewerbsrechts und zur Förderung des Wettbewerbs auf digitalen Märkten; und

(c) alle sonstigen von den Vertragsparteien vereinbarten Formen der technischen Zusammenarbeit.

2. In Bereichen von gemeinsamem Interesse und vorbehaltlich der verfügbaren Ressourcen jeder Vertragspartei sind die Vertragsparteien bestrebt, in Fragen der Durchsetzung des Wettbewerbsrechts in digitalen Märkten nach Möglichkeit und in Übereinstimmung mit ihren jeweiligen Gesetzen und sonstigen Vorschriften zusammenzuarbeiten, namentlich durch Notifikationen, Konsultationen und den Austausch von Informationen.

Art. 36-U Digitale Identitäten

Die Vertragsparteien anerkennen, dass die Zusammenarbeit im Bereich der digitalen Identitäten die regionale und globale Konnektivität erhöhen kann und dass jede Vertragspartei unterschiedliche rechtliche und technische Ansätze für digitale Identitäten verfolgen kann. Zur Förderung der Kompatibilität können die Vertragsparteien Initiativen von gemeinsamem Interesse ergreifen, die Folgendes umfassen können:

(a) die Entwicklung geeigneter Rahmenwerke und gemeinsamer Standards zur Förderung der technischen Interoperabilität zwischen der Art und Weise, wie digitale Identitäten durch die einzelnen Vertragsparteien umgesetzt werden;

(b) die Entwicklung eines vergleichbaren Schutzes digitaler Identitäten innerhalb des jeweiligen Rechtsrahmens jeder Vertragspartei oder die Anerkennung ihrer rechtlichen Wirkungen, unabhängig davon, ob sie autonom oder durch Vereinbarung gewährt wird;

(c) die Unterstützung der Entwicklung internationaler Rahmenwerke zu Systemen für digitale Identitäten;

(d) die Umsetzung von Anwendungsfällen für die gegenseitige Anerkennung digitaler Identitäten; und

(e) den Austausch von Wissen und Fachkenntnissen über Best Practices in Bezug auf politische Strategien und Vorschriften für digitale Identitäten, technische Umsetzungs- und Sicherheitsstandards sowie zur Förderung der Nutzung digitaler Identitäten.

Art. 36-V Zusammenarbeit im Bereich Finanztechnologie (FinTech)

Die Vertragsparteien anerkennen, wie wichtig die Zusammenarbeit zwischen ihren FinTech-Branchen ist und dass für eine wirksame Zusammenarbeit in diesem Bereich

die Einbeziehung der Unternehmen notwendig ist. Zu diesem Zweck unterstützen die Vertragsparteien:

(a) die Zusammenarbeit von Unternehmen im FinTech-Sektor;

(b) die Entwicklung von FinTech-Lösungen für den Unternehmens- oder den Finanzsektor; und

(c) die Zusammenarbeit von Top-Talenten oder Start-ups im FinTech-Bereich in Übereinstimmung mit den Gesetzen und sonstigen Vorschriften der Vertragsparteien.

Art. 36-W Künstliche Intelligenz

1. Die Vertragsparteien anerkennen, dass die Verwendung und Einführung von Technologien der künstlichen Intelligenz («KI») in der digitalen Wirtschaft zunehmend an Bedeutung gewinnt und dass KI für Personen und Unternehmen erhebliche soziale und wirtschaftliche Vorteile bietet. Gleichzeitig anerkennen die Vertragsparteien, dass KI-Technologien neue Herausforderungen und Risiken mit sich bringen, auf die angemessen reagiert werden muss. Die Vertragsparteien können in Übereinstimmung mit ihrer entsprechenden politischen Strategie zusammenarbeiten, indem sie:

(a) sich über KI-bezogene Initiativen sowie über Forschungsergebnisse und Branchenpraktiken im Zusammenhang mit KI-Technologien und deren Governance austauschen;

(b) die verantwortungsvolle Nutzung und Einführung von KI-Technologien durch Unternehmen und die gesamte Gemeinschaft fördern und unterstützen;

(c) kommerzielle Chancen und Kooperationen zwischen Forschung, Hochschulen und der Branche fördern; und

(d) Möglichkeiten für gemeinsame KI-Projekte und Initiativen für den Einsatz von oder Testumgebungen für KI zwischen den Vertragsparteien prüfen.

2. Die Vertragsparteien anerkennen, dass es für die ethische, vertrauenswürdige, sichere und verantwortungsvolle Entwicklung und Nutzung von KI regulatorische und politische Rahmenwerke sowie entsprechende Standards braucht, die die Interoperabilität fördern und einschlägige internationale Grundsätze, Leitlinien und Standards berücksichtigen, und dass solche Rahmenwerke und Standards dazu beitragen werden, die Vorteile dieser Technologien zu nutzen. Zu diesem Zweck anerkennen die Vertragsparteien, wie wichtig es ist:

(a) die Grundsätze, Leitlinien und Standards der einschlägigen internationalen Gremien zu berücksichtigen;

(b) für die Rahmenwerke und die Regulierung risikobasierte Ansätze anzuwenden, die sich auf von der Branche ausgehende Standards und Best Practices im Bereich Risikomanagement stützen; und

(c) den Grundsätzen der technologischen Interoperabilität und der Technologieneutralität Rechnung zu tragen.

Art. 36-X Standards, technische Vorschriften und Konformitätsbewertungsverfahren

1. Die Vertragsparteien fördern gegebenenfalls die Einführung von internationalen oder international anerkannten Standards für die digitale Wirtschaft. In aufkommenden Bereichen der digitalen Wirtschaft von gemeinsamem Interesse sollen die Vertragsparteien, soweit angebracht, zudem:

(a) an internationalen Gremien, denen alle Vertragsparteien angehören, teilnehmen und darin zusammenarbeiten, um die Entwicklung von Standards zu fördern; und

(b) in Bereichen ohne entsprechende Standards gemeinsam Zusammenarbeitsmöglichkeiten prüfen, um von den anderen Vertragsparteien entwickelte Standards anzuerkennen.

2. Die Vertragsparteien anerkennen, dass Mechanismen, mit denen die grenzüberschreitende Anerkennung von Konformitätsbewertungsergebnissen erleichtert wird, die digitale Wirtschaft unterstützen können.

3. In Bereichen der digitalen Wirtschaft von gemeinsamem Interesse sollen die Vertragsparteien:

(a) gemeinsame Initiativen in Bezug auf Standards und Konformitätsbewertungen ermitteln und diesbezüglich zusammenarbeiten;

(b) gegebenenfalls etablierte internationale Vereinbarungen über die gegenseitige Anerkennung von Akkreditierungen anwenden;

(c) Vorschläge einer anderen Vertragspartei zur Zusammenarbeit bei Standards, technischen Vorschriften und Konformitätsbewertungsverfahren wohlwollend prüfen; und

(d) die Zusammenarbeit zwischen dem öffentlichen Sektor und der Privatwirtschaft fördern, einschliesslich grenzüberschreitender Forschungs- und Testprojekte, um zwischen den Vertragsparteien und der Branche ein besseres Verständnis der Standards, technischen Vorschriften und Konformitätsbewertungsverfahren zu entwickeln.

4. Die Vertragsparteien anerkennen, wie wichtig der Informationsaustausch und Transparenz im Hinblick auf die Ausarbeitung, Einführung und Anwendung von Standards, technischen Vorschriften und Konformitätsbewertungsverfahren mit Bezug zur digitalen Wirtschaft ist. Jede Vertragspartei ist bestrebt, auf Ersuchen einer anderen Vertragspartei innerhalb einer angemessenen Frist, die zwischen der ersuchenden und der ersuchten Vertragspartei vereinbart wird, und nach Möglichkeit innerhalb von 60 Tagen nach dem Ersuchen Informationen über Standards, technische Vorschriften und Konformitätsbewertungsverfahren mit Bezug zur digitalen Wirtschaft zur Verfügung zu stellen.

Art. 36-Y Innovation

Die Vertragsparteien anerkennen, wie wichtig die Digitalisierung und die Nutzung neuer Technologien für die digitale Wirtschaft ist, einschliesslich der Distributed-

Ledger-Technologie und ihrer Anwendungsfälle bei der Tokenisierung von Vermögenswerten, da dies zum Wirtschaftswachstum und zur wirtschaftlichen Entwicklung beiträgt. Darüber hinaus anerkennen die Vertragsparteien die Notwendigkeit eines experimentier- und innovationsfreundlichen Umfelds, um den elektronischen Handel zu unterstützen und die digitale Wirtschaft zu fördern, einschliesslich durch:

(a) die Ermittlung relevante Ansätze und Technologien zur Ermöglichung grenzüberschreitender Datenflüsse;

(b) die Zusammenarbeit bei der Entwicklung von politischen Rahmenwerken und Referenzanwendungsfällen; und

(c) den Austausch über die Forschung und über Branchenpraktiken mit Bezug zur Innovation.

Art. 36-Z Kleine und mittlere Unternehmen

1. Die Vertragsparteien anerkennen die grundlegende Rolle der kleinen und mittleren Unternehmen (KMU) zur Beibehaltung der Dynamik und zur Stärkung der Wettbewerbsfähigkeit in der digitalen Wirtschaft.

2. Die Vertragsparteien fördern die Zusammenarbeit zwischen ihren KMU in Bezug auf die digitale Wirtschaft.

3. Im Hinblick auf eine intensivere Zusammenarbeit zwischen den Vertragsparteien zur Verbesserung der Handels- und Investitionsmöglichkeiten für KMU in der digitalen Wirtschaft können die Vertragsparteien:

(a) weiterhin mit den anderen Vertragsparteien zusammenarbeiten, um Informationen und Best Practices für einen wirksameren Einsatz digitaler Instrumente und Technologien auszutauschen und dadurch die Beteiligung von KMU an der digitalen Wirtschaft zu verbessern; und

(b) die Beteiligung der KMU der Vertragsparteien an Plattformen fördern, die dazu beitragen könnten, KMU mit internationalen Anbietern, Abnehmern und anderen potenziellen Geschäftspartnern zusammenzubringen.

Art. 36-AA Digitale Inklusion

1. Die Vertragsparteien anerkennen, wie wichtig die digitale Inklusion ist, damit sichergestellt werden kann, dass allen Personen und Unternehmen alles Notwendige zur Verfügung steht, um an der digitalen Wirtschaft teilzuhaben, zu ihr beizutragen und von ihr zu profitieren.

2. Die Vertragsparteien anerkennen, wie wichtig es ist, durch die Beseitigung von Hindernissen die sich durch die digitale Wirtschaft bietenden Möglichkeiten zu erweitern und zu erleichtern. Dies kann gegebenenfalls die Stärkung kultureller und völkerübergreifender Beziehungen, einschliesslich zwischen indigenen Völkern, sowie die Verbesserung des Zugangs für Frauen, ländliche Regionen, junge und ältere Menschen, Menschen mit Beeinträchtigungen und sozioökonomisch benachteiligte Gruppen umfassen.

3. Die Vertragsparteien können wie folgt zusammenarbeiten:

(a) Austausch von Erfahrungen und Best Practices in Bezug auf digitale Inklusion, einschliesslich Expertenaustausch;

(b) Förderung eines inklusiven und nachhaltigen Wirtschaftswachstums, um dazu beizutragen, dass die Vorteile der digitalen Wirtschaft breiteren Bevölkerungsgruppen zugänglich sind;

(c) Beseitigung von Hindernissen für den Zugang zu digitalen Geschäftsmöglichkeiten;

(d) Entwicklung von Programmen zur Förderung der Teilhabe aller Gruppen an der digitalen Wirtschaft;

(e) Möglichkeiten für «neue» Arbeitsformen wie Telearbeit oder Co-Working;

(f) Austausch und gemeinsame Nutzung von Methoden und Verfahren für die Beschaffung nicht aggregierter Daten, die Nutzung von Indikatoren und die Analyse von Statistiken über die Beteiligung an der digitalen Wirtschaft; und

(g) in weiteren von den Vertragsparteien gemeinsam vereinbarten Bereichen.

4. Tätigkeiten im Rahmen der Zusammenarbeit auf dem Gebiet der digitalen Inklusion können gegebenenfalls durch die Koordination unter anderem zwischen den jeweiligen Stellen, Unternehmen, Gewerkschaften, der Zivilgesellschaft, akademischen Institutionen und Nichtregierungsorganisationen der Vertragsparteien durchgeführt werden.

Art. 36-AB Allgemeine Ausnahmen

1. Für die Zwecke dieses Kapitels finden Artikel XX des GATT 1994[15] und die Hinweise zu seiner Auslegung sowie Artikel XIV Buchstaben a–c des GATS[16] Anwendung und werden hiermit *mutatis mutandis* zu Bestandteilen dieses Abkommens erklärt.

2. Die Vertragsparteien kommen überein, dass die Massnahmen nach Artikel XX Buchstabe b des GATT 1994 Umweltmassnahmen zum Schutz des Lebens und der Gesundheit von Menschen, Tieren und Pflanzen einschliesst und dass Artikel XX Buchstabe g des GATT 1994 für Massnahmen zur Erhaltung lebender und nichtlebender erschöpfbarer natürlicher Ressourcen gilt.

Art. 36-AC Ausnahmen aus Gründen der Sicherheit

Die Artikel 20 und 34 finden sinngemäss Anwendung auf dieses Kapitel.

Art. 36-AD Schutz kritischer öffentlicher Infrastrukturen

1. Keine Bestimmung dieses Kapitels soll dahin ausgelegt werden, dass eine Vertragspartei daran gehindert wird, Massnahmen zu treffen, die sie zum Schutz ihrer

15 SR **0.632.20**, Anhang 1A.1
16 SR **0.632.20**, Anhang 1B

wesentlichen Sicherheitsinteressen als erforderlich erachtet, namentlich um ihre kritischen öffentlichen Infrastrukturen wie Kommunikations-, Energie-, Wasser- und Transportinfrastrukturen, die lebenswichtige Güter oder Dienstleistungen bereitstellen, vor vorsätzlichen Versuchen zu schützen, diese ausser Betrieb zu setzen oder zu beschädigen.

2. Im Interesse grösserer Rechtssicherheit sei darauf hingewiesen, dass dieser Artikel die Auslegung anderer in diesem Abkommen vorgesehener Ausnahmen oder das Recht einer Vertragspartei, eine davon in Anspruch zu nehmen, nicht berührt.

Art. 36-AE Aufsichtsrechtliche Massnahmen

1 Keine Bestimmung dieses Kapitels soll dahin ausgelegt werden, dass eine Vertragspartei daran gehindert wird, aus aufsichtsrechtlichen Gründen angemessene Massnahmen einzuführen oder aufrechtzuerhalten, etwa:

(a) zum Schutz von Investorinnen und Investoren, Einlegerinnen und Einlegern, Versicherungsnehmenden, anspruchsberechtigten Versicherten, von Personen, gegenüber denen ein Finanzdienstleistungserbringer treuhänderische Pflichten hat, und von gleichartigen Teilnehmerinnen und Teilnehmern am Finanzmarkt;

(b) zur Wahrung der Sicherheit, Solidität, Integrität oder finanziellen Verantwortung von Finanzdienstleistungserbringern; und

(c) zur Gewährleistung der Integrität und Stabilität des Finanzsystems einer Vertragspartei.

2. Diese Massnahmen dürfen nicht belastender sein, als zur Erreichung ihrer Ziele erforderlich ist, und dürfen keine willkürliche oder ungerechtfertigte Diskriminierung gegenüber Finanzdienstleistungserbringern einer anderen Vertragspartei im Vergleich zu eigenen gleichen Finanzdienstleistungserbringern oder eine versteckte Beschränkung des Dienstleistungshandels darstellen.

3. Keine Bestimmung dieses Kapitels soll dahin ausgelegt werden, dass eine Vertragspartei dazu verpflichtet wird, Informationen über die Geschäfte und Konten einzelner Konsumentinnen und Konsumenten offenzulegen oder vertrauliche oder geschützte Informationen preiszugeben, die sich im Besitz öffentlicher Stellen befinden.

4. Jede Vertragspartei unternimmt alle möglichen Anstrengungen, um sicherzustellen, dass die «Grundsätze für eine wirksame Bankenaufsicht» des Basler Ausschusses für Bankenaufsicht, die Standards und Grundsätze der Internationalen Vereinigung der Versicherungsaufseher (IAIS) sowie die Ziele und Prinzipien der Effektenhandelsaufsicht (*Objectives and Principles of Securities Regulation*) der Internationalen Organisation der Wertpapieraufsichtsbehörden (IOSCO) auf ihrem Hoheitsgebiet umgesetzt und eingehalten werden.

Art. 36-AF Spezifische Ausnahmen

1. Keine Bestimmung dieses Kapitels soll dahin ausgelegt werden, dass eine Vertragspartei einschliesslich ihrer öffentlichen Stellen an der alleinigen Ausübung von

Tätigkeiten oder an der alleinigen Erbringung von Dienstleistungen in ihrem Hoheitsgebiet gehindert wird, die Teil einer staatlichen Alterssicherung oder eines gesetzlichen Systems der sozialen Sicherheit sind.

2. Keine Bestimmung dieses Kapitels soll dahin ausgelegt werden, dass eine Vertragspartei einschliesslich ihrer öffentlichen Stellen an der alleinigen Ausübung von Tätigkeiten oder der alleinigen Erbringung von Dienstleistungen in ihrem Hoheitsgebiet gehindert wird, die auf staatliche Rechnung oder mit staatlicher Garantie oder unter Verwendung staatlicher Finanzmittel dieser Vertragspartei oder ihrer öffentlichen Stellen ausgeübt oder erbracht werden.

3. Lässt eine Vertragspartei zu, dass eine der in den Absätzen 1 oder 2 genannten Tätigkeiten oder Dienstleistungen von seinen Finanzdienstleistungserbringern im Wettbewerb mit einer öffentlichen Stelle oder einem Finanzdienstleistungserbringer ausgeübt oder erbracht wird, so umfasst der Begriff «Dienstleistungen» auch solche Tätigkeiten.

4. Keine Bestimmung dieses Kapitel gilt für Tätigkeiten oder Dienstleistungen, die von einer Zentralbank oder einer Währungsbehörde oder einer sonstigen öffentlichen Stelle im Rahmen der Geld- oder Währungspolitik ausgeübt oder erbracht werden.

Art. 36-AG Besteuerung

1. Keine Bestimmung dieses Kapitel gilt für Steuern oder fiskalische Massnahmen.[17]

2. Keine Bestimmung dieses Kapitels berührt die Rechte und Pflichten einer Vertragspartei aus einem Steuerabkommen. Im Falle einer Unvereinbarkeit zwischen diesem Kapitel und einem solchen Steuerabkommen hat bezüglich dieser Unvereinbarkeit Letzteres Vorrang. Es obliegt allein den nach dem betreffenden Steuerabkommen zuständigen Behörden, festzulegen, ob zwischen diesem Kapitel und dem Steuerabkommen eine Unvereinbarkeit besteht.

[17] Steuern und fiskalische Massnahmen umfassen auch Verbrauchssteuern, aber keine Zölle nach Artikel 8 Absatz 2 dieses Abkommens.

Anhang II

Artikel 5bis

Art. 5bis Standort von Rechenanlagen für Finanzdienstleistungen

1. Für die Zwecke dieses Artikels bedeutet «Rechenanlagen» Computerserver und Speichergeräte zur Bearbeitung oder Speicherung von Informationen für kommerzielle Zwecke, nicht jedoch Computerserver oder Speichervorrichtungen von oder für den Zugang zu Finanzmarktinfrastrukturen.

2. Die Vertragsparteien anerkennen, dass jede Vertragspartei ihre eigenen regulatorischen Anforderungen hinsichtlich der Nutzung von Rechenanlagen haben kann, einschliesslich Anforderungen, mit denen die Sicherheit und Vertraulichkeit der Kommunikation gewährleistet werden soll.

3. Keine Vertragspartei verlangt von einem Finanzdienstleistungserbringer, dass er als Voraussetzung für die Ausübung einer Geschäftstätigkeit in ihrem Hoheitsgebiet Rechenanlagen in diesem Hoheitsgebiet nutzt oder errichtet, sofern die Finanzregulierungs- oder -aufsichtsbehörden der Vertragspartei rechtzeitig Zugang zu den für die Erfüllung ihrer Aufsichtsaufgaben erforderlichen Daten erhalten. Zu diesem Zweck darf eine Vertragspartei keine Massnahmen einführen oder aufrechterhalten, die die grenzüberschreitende Datenübermittlung verbieten oder beschränken, indem sie:

(a) die Nutzung von Rechenanlagen oder Netzelementen im Hoheitsgebiet der Vertragspartei für die Datenbearbeitung vorschreibt, auch durch die Vorgabe der Nutzung von Rechenanlagen oder Netzelementen, die im Hoheitsgebiet der Vertragspartei zertifiziert oder zugelassen sind;

(b) die Lokalisierung von Daten im Hoheitsgebiet der Vertragspartei zur Speicherung oder Bearbeitung verlangt;

(c) die Speicherung oder Datenbearbeitung im Hoheitsgebiet einer anderen Vertragspartei verbietet;

(d) die grenzüberschreitende Datenübermittlung von der Nutzung von Rechenanlagen oder Netzelementen im Hoheitsgebiet der Vertragspartei oder von Lokalisierungsanforderungen im Hoheitsgebiet der Vertragspartei abhängig macht; oder

(e) die Datenübermittlung in das Hoheitsgebiet der Vertragspartei verbietet.

4. Im Interesse grösserer Rechtssicherheit ist Artikel 4 dieses Abkommens auf Absatz 3 dieses Artikels anwendbar.

5. Die Vertragsparteien überprüfen die Durchführung dieser Bestimmung und bewerten ihr Funktionieren innerhalb von drei Jahren nach dem Inkrafttreten des am 25. September 2025 in Bern, Schweiz, zwischen den EFTA-Staaten und Singapur abgeschlossenen Abkommens über die digitale Wirtschaft. Eine Vertragspartei kann den anderen Vertragsparteien jederzeit vorschlagen, die Liste der in Absatz 3 aufgeführten Beschränkungen zu überprüfen, auch wenn sie selbst oder eine andere Vertragspartei

vereinbart hat, in einem künftigen bilateralen oder multilateralen Abkommen keine anderen Arten von Massnahmen einzuführen oder aufrechtzuerhalten, die über die in Absatz 3 aufgeführten Massnahmen hinausgehen. Ein solches Ersuchen wird wohlwollend geprüft.