Referentenentwurf

des Bundesministeriums für Digitales und Verkehr

Entwurf eines ersten Gesetzes zur Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes

A. Problem und Ziel

Die elektronische Kommunikation über E-Mail, Chat- oder Messenger-Dienste und die Nutzung von Clouddiensten sind gegenüber der herkömmlichen nummerngebundenen Sprachtelefonie von immer größer werdender Bedeutung für den privaten wie beruflichen Austausch und die Speicherung von Informationen. Bei nummernunabhängigen interpersonellen Telekommunikationsdiensten ist die sichere Ende-zu-Ende-Verschlüsselung inzwischen Branchenstandard. Geeignete Verschlüsselungstechnologien sind vorhanden, werden aber nicht durchgängig von Anbietern dieser Dienste bereitgestellt.

Mit der Ergänzung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) sollen nummernunabhängige interpersonelle Telekommunikationsdienste dazu verpflichtet werden, ihre Telekommunikationsdienste als Standard mit einer Ende-zu-Ende-Verschlüsselung anzubieten. Das Gleiche gilt für die Speicherung von Informationen im Rahmen der Nutzung von Cloud-Diensten, die von den meisten Wirtschaftsunternehmen sowie einem immer größer werdenden Anteil von Bürgerinnen und Bürgern in Anspruch genommen werden. Das Recht auf Verschlüsselung trägt dazu bei, die Akzeptanz für verbreitete Anwendung von Verschlüsselungstechnologien in der Bevölkerung, Wirtschaft wie auch öffentlichen Institutionen zu erhöhen. Es handelt sich um einen essentiellen Beitrag zur Gewährleistung der Grundrechte auf Gewährleistung des Fernmeldegeheimnisses sowie der Vertraulichkeit und Integrität informationstechnischer Systeme und zur Cybersicherheit.

Der Gesetzentwurf dient darüber hinaus auch zur Vornahme von klarstellenden und ergänzenden Regelungen im Bereich der Regelungen zur Aufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und die Bundesnetzagentur (BNetzA) sowie die Befugnisse zur Verarbeitung von Verkehrs-, Standort-, Bestands- und Nutzungsdaten zur Erfüllung der Pflichten nach der Verordnung (EU) 2023/1543.

B. Lösung

Einfügung eines Rechts auf Verschlüsselung in das Telekommunikation-Telemedien-Datenschutz-Gesetz.

C. Alternativen

Keine. Ein Recht auf Verschlüsselung bedarf einer gesetzlichen Regelung.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keiner.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für Bürgerinnen und Bürger

E.2 Erfüllungsaufwand für die Wirtschaft

Ende-zu-Ende-Verschlüsselung wird bereits von vielen betroffenen Diensteanbietern standardmäßig bereitgehalten, so dass mit einem Recht auf sichere Ende-zu-Ende-Verschlüsselung kein nennenswerter Erfüllungsaufwand einhergehen dürfte. Demgegenüber legt die Wirtschaft großen Wert auf die Gewährleistung einer sicheren Ende-zu-Ende-Verschlüsselung und sieht dies als einen Grundpfeiler des Wirtschaftsstandorts Deutschland an.

Davon Bürokratiekosten aus Informationspflichten

Es ist vorgesehen, dass die betroffenen Anbieter ihre Nutzer über die Durchführung einer Ende-zu-Ende-Verschlüsselung oder darüber, wie den Nutzern eine Ende-zu-Ende-Verschlüsselung ermöglicht wird, informieren müssen. Im Hinblick auf die ohnehin umfangreichen Nutzerinformationen, die von den Anbietern bereitgestellt werden, dürfte der mit dieser Information verbundene Aufwand gering sein.

E.3 Erfüllungsaufwand der Verwaltung

Noch zu ergänzen: es entstehen zusätzliche Aufgaben der BNetzA im Bereich der Aufsicht, hinsichtlich der Ermöglichung der Ende-zu-Ende-Verschlüsselung durch betroffene Telekommunikationsanbieter.

F. Weitere Kosten

Sonstige Kosten für die Wirtschaft, für soziale Sicherungssysteme, Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau sind nicht zu erwarten.

Referentenentwurf des Bundesministeriums für Digitales und Verkehr

Entwurf eines ersten Gesetzes zur Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes[*)]

Das Telekommunikation-Telemedien-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 4 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544; 2022 I 1045) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Nach § 13 wird eingefügt: „§ 13 a Erfüllung von Pflichten gemäß Artikel 10 und 11 der Verordnung (EU) 2023/1543“.

   b) Nach § 24 wird eingefügt: „§ 24a Erfüllung von Pflichten gemäß Artikel 10 und 11 der Verordnung (EU) 2023/1543“

2. In § 2 Absatz 2 werden folgende Nummern 7 und 8 angefügt:

   „7. „sichere Ende-zu-Ende-Verschlüsselung“ eine Verschlüsselungstechnologie, durch die ein Telekommunikationsinhalt beim absendenden Endnutzer verschlüsselt und erst beim empfangenden Endnutzer wieder entschlüsselt wird, so dass er über den gesamten Übertragungsweg unlesbar ist, nicht eingesehen werden kann und auch der Anbieter des Telekommunikationsdienstes oder Dritte nicht an den Schlüssel gelangen können.

   8. „Teilnehmerdaten“ Daten gemäß Artikel 3 Nummer 9 der Verordnung (EU) 2023/1543.“

3. In § 3 wird folgender Absatz 5 angefügt:

   „(5) Anbieter von nummernunabhängigen interpersonellen Telekommunikationsdiensten im Sinne von § 3 Nummer 40 des Telekommunikationsgesetzes führen eine sichere Ende-zu-Ende-Verschlüsselung durch oder gewährleisten, dass Endnutzer ihre Telekommunikationsinhalte mit einer Ende-zu-Ende-Verschlüsselung versehen können. Endnutzer sind über die Durchführung der sicheren Ende-zu-Ende-Verschlüsselung

---

[*)] Die Verpflichtungen aus der Richtlinie EU/2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. EG Nr. L 241 S. 1 vom 17.09.2015) sind beachtet worden.

durch den Anbieter des Telekommunikationsdienstes oder darüber, wie eine Ende-zu-Ende-Verschlüsselung möglich ist, zu informieren. Für den Fall, dass eine sichere Ende-zu-Ende-Verschlüsselung technisch nicht möglich ist, informiert der Anbieter des Telekommunikationsdienstes über die technischen Gründe, die einer sicheren Ende-zu-Ende-Verschlüsselung entgegenstehen."

4. Nach § 13 wird folgender § 13a eingefügt:

   „§ 13a Erfüllung von Pflichten gemäß Artikel 10 und 11 der Verordnung (EU) 2023/1543

   Anbieter von gewerblich angebotenen Telekommunikationsdiensten dürfen Teilnehmerdaten, Verkehrsdaten nach § 9 sowie Standortdaten nach § 13 verarbeiten, soweit dies zur Sicherung und Übermittlung elektronischer Beweismittel im Falle einer Europäischen Herausgabeanordnung oder zur Sicherung der Daten im Falle einer Europäischen Sicherungsanordnung gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren erforderlich ist.."

5. In § 19 wird folgender Absatz 6 angefügt:

   „(6) „Anbieter von Telemedien, deren Dienstleistung darin besteht, vom Nutzer von Telemedien bereitgestellte Informationen für diesen auf einem Datenspeicher zum Abruf bereitzuhalten, informieren den Nutzer über die Möglichkeit einer durchgehenden und sicheren Verschlüsselung der bereitgestellten Informationen, die gewährleistet, dass die Informationen nur vom bereitstellenden Nutzer gelesen werden können."

6. Nach § 24 wird folgender § 24a eingefügt:

   „§ 24a Erfüllung von Pflichten gemäß Artikel 10 und 11 der Verordnung (EU) 2023/1543

   Anbieter von gewerblich angebotenen Telemedien, die es ihren Nutzern ermöglichen, miteinander zu kommunizieren oder Daten zu speichern oder auf sonstige Weise zu verarbeiten, sofern die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist, sowie Anbieter von Internetdomänennamen- und IP-Nummerierungsdiensten wie Diensten der IP-Adressenzuweisung und der Domänennamen-Registrierung, Anbieter von Domänennamen-Registrierungsstellendienste und Anbieter von mit Domänennamen verbundenen Datenschutz- und Proxy-Diensten dürfen Teilnehmerdaten und Nutzungsdaten verarbeiten, soweit dies zur Sicherung und Übermittlung elektronischer Beweismittel im Falle einer Europäischen Herausgabeanordnung oder zur Sicherung der Daten im Falle einer Europäischen Sicherungsanordnung gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren erforderlich ist."

7. § 28 wird wie folgt geändert:

   a) In Absatz 1 wird die Angabe „1." durch die Angabe „1a" ersetzt. Vor Nummer „1a)" wird folgende Nummer 1 eingefügt:

      „1. entgegen § 3 Absatz 5 Satz 2 und 3 Endnutzer nicht informiert,"

   b) In Absatz 1 wird nach Nummer 10 folgende Nummer 10a eingefügt:

„10a. entgegen § 19 Absatz 6 den Nutzer nicht informiert.

c) In Absatz 3 wird die Angabe „Nummer 1 und 9“ durch die Angabe „Nummer 1, 1a und 9“ ersetzt.

8. § 29 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist die zuständige Aufsichtsbehörde über die Einhaltung der gesetzlichen Anforderungen an die Verarbeitung von Teilnehmerdaten, Verkehrs- und Standortdaten gemäß §§ 9, 10, 12, 13 und 13a.“

b) In Absatz 2 wird nach dem Wort „Telekommunikationsdiensten“ folgendes eingefügt: „, Postdiensten“.

c) In Absatz 3 wird folgender Satz angefügt:

„Insbesondere kann der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

1. Anordnungen und andere Maßnahmen treffen, um die Einhaltung des Datenschutzes sicherzustellen,

2. vom Verpflichteten Auskunft verlangen,

3. zur Überprüfung der Einhaltung der Verpflichtungen Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten betreten und besichtigen,

4. bei Nichterfüllung von Datenschutzverpflichtungen den Betrieb von betroffenen Telekommunikationsanlagen oder das Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen und

5. zur Durchsetzung von Maßnahmen und Anordnungen nach den Nummern 1 bis 4 nach Maßgabe des Verwaltungsvollstreckungsgesetzes ein Zwangsgeld bis zu 1 Million Euro festsetzen.“

9. In § 30 wird folgender Absatz 6 angefügt:

„(6) Zur Durchsetzung des Verbotes nach § 8 kann die Bundesnetzagentur von Anbietern von Online-Plattformen, die für den Handel mit verbotenen Telekommunikationsanlagen genutzt werden, Auskunft über personenbezogene Daten von Verkäufern und Käufern verlangen, soweit dies für den Vollzug dieses Gesetzes erforderlich ist.“

Artikel 2

Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am 1. April 2025 in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

1. Ende-zu-Ende-Verschlüsselung bei nummernunabhängigen interpersonellen Telekommunikationsdiensten

Die nummernunabhängigen interpersonellen Telekommunikationsdienste, d. h. E-Mail-Dienste, Messengerdienste und Chat-Dienste erfahren heute eine breite Nutzung sowohl im privaten wie auch im beruflichen Bereich. Sie unterliegen uneingeschränkt der Vertraulichkeit der Kommunikation (EU-Ebene) bzw. dem Fernmeldegeheimnis in Deutschland. Während eine Ende-zu-Ende-Verschlüsselung bei nummerngebundenen interpersonellen Telekommunikationsdiensten (§ 3 Nummer 37 Telekommunikationsgesetz) technisch nicht möglich ist, ist die Ende-zu-Ende-Verschlüsselung, soweit sie technisch möglich ist, bei nummernunabhängigen interpersonellen Telekommunikationsdiensten – insbesondere den Messengerdiensten, ein Bestandteil des Schutzes der Vertraulichkeit der Kommunikation. Sie dient dem Schutz der Privatsphäre wie auch zum Schutz von Berufs- und Geschäftsgeheimnissen. Die Ende-zu-Ende-Verschlüsselung sichert die Verschlüsselung durchgehend von Endnutzer zu Endnutzer und verhindert, dass sich der Anbieter oder Dritte auf den Servern, die während der Übertragung als Zwischenstationen dienen, von einem Kommunikationsinhalt Kenntnis von Kommunikationsinhalten verschaffen können. Ein Recht der Endnutzer auf Ende-zu-Ende-Verschlüsselung besteht derzeit nicht. Da die Ende-zu-Ende-Verschlüsselung eine vorhandene Technologie zur Gewährleistung der Vertraulichkeit der Kommunikation darstellt, dient sie zugleich dem grundrechtlich geschützten Fernmeldegeheimnis. Endnutzer sollten daher das Recht haben diese Dienste mit einer Ende-zu-Ende-Verschlüsselung nutzen zu können, soweit dies technisch möglich ist.

Das Bundeskartellamt (BKartA) hat am 17. Mai 2023 seinen Abschlussbericht zur Sektoruntersuchung bezüglich Messenger- und Videodiensten veröffentlicht und darin einen besonderen Schwerpunkt auf Datenschutz- und Datensicherheitsfragen – insbesondere auf das Thema Ende-zu-Ende-Verschlüsselung - gelegt (vgl. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/17_05_2023_SU_MD.html und https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_MessengerVideoDienste.pdf;jsessionid=E4954BD5863FB199ED993B6FD2906D4E.1_cid381?__blob=publicationFile&v=5).

Nach den Erkenntnissen aus dem Abschlussbericht des BKartA ergibt sich folgendes Bild:

Obwohl die Ende-zu-Ende-Verschlüsselung inzwischen Branchenstandard ist, setzen einzelne Messenger-Dienste die Ende-zu-Ende-Verschlüsselung nicht oder nur bei bestimmten Funktionen ein, ohne dass das mit technischen Restriktionen begründet werden kann. Zudem sieht das BKartA eine mögliche Irreführung der Verbraucherinnen und Verbraucher durch unklare Informationen, etwa ob eine Ende-zu-Ende-Verschlüsselung automatisch erfolgt, der Endnutzer sie erst aktivieren muss oder ob sie auf bestimmte Funktionen beschränkt ist und welche das sind.

Technische Einschränkungen bestehen bei Videokonferenzen und Webinaren, weil die Ende-zu-Ende-Verschlüsselung erfordert, dass die Teilnehmenden technisch in der Lage sind, die notwendigen Verschlüsselungsfunktionen bereitzustellen und anzuwenden. Eine Ende-zu-Ende-Verschlüsselung kann nach den Erkenntnissen des BKartA nicht erreicht

werden, sobald einzelne Teilnehmerinnen oder Teilnehmer hinter dem dafür geforderten Sicherheitsniveau zurückbleiben.

Das BkartA geht weiterhin davon aus, dass die Ende-zu-Ende-Verschlüsselung bei Verwendung bestimmter Funktionen (Teilnahme über einen nummerngebundenen Telekommunikationsdienst oder die Aufzeichnung der Konferenz durch den anbietenden Dienst) technisch nicht möglich ist. Auch bei Anbindung etwa von Geräten, die auf dem SIP-Protokoll (Session Initiation Protocol - Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern) basieren, ist nach den Erkenntnissen des BKartA Ende-zu-Ende-Verschlüsselung nicht möglich, da dazu die verschiedenen Protokolle synchronisiert werden müssten.

Auch die meisten anderen Dienste, die eine Kommunikation in Gruppen anbieten, können dabei eine Ende-zu-Ende-Verschlüsselung wegen des damit verbundenen Aufwandes nicht sicherstellen .

2. Ende-zu-Ende-Verschlüsselung und Interoperabilität

Das BKartA sieht keinen technischen Ansatz für eine marktweit interoperable Ende-zu-Ende-Verschlüsselung. Die Interoperabilität wird von der Verordnung (EU) 2022/1925 über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) für bestimmte Dienste, die nach der Verordnung als sogenannte „Gatekeeper“ oder „Torwächter“ anzusehen sind, gefordert. Sie bezeichnet gemäß Artikel 2 Nummer 29 des Gesetzes über digitale Märkte die Fähigkeit, Informationen auszutauschen und die über Schnittstellen oder andere Lösungen ausgetauschten Informationen beiderseitig zu nutzen, sodass alle Hardware- oder Softwarekomponenten mit anderer Hardware und Software auf die vorgesehene Weise zusammenwirken und bei Nutzern auf die vorgesehene Weise funktionieren. Das ist für die Ende-zu-Ende-Verschlüsselung eine Herausforderung und umgekehrt. Das Gesetz über digitale Märkte legt in Artikel 7 (Verpflichtungen von Torwächtern zur Interoperabilität nummernunabhängiger interpersoneller Kommunikationsdienste) fest, dass das Sicherheitsniveau einschließlich der Ende-zu-Ende-Verschlüsselung, die der Torwächter seinen eigenen Endnutzern bietet, bei allen interoperablen Diensten beibehalten werden muss.

3. Verschlüsselung von Informationen bei Clouddiensten

Das Recht auf auf eine sichere und durchgängige Verschlüsselung von Informationen muss auch Informationen umfassen, die von Nutzern bei externen Dienstleistern für den Nutzer verarbeitet werden und die dort nur für berechtigte Nutzer, nicht aber für die Öffentlichkeit zur Verfügung stehen. Die Spannbreite der Cloud-Dienste umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Anwendungen. Das Recht auf Verschlüsselung wird hier für solche Clouddienste geregelt, die als Speicherdienste fungieren, die von den meisten Unternehmen, aber auch von Bürgerinnen und Bürgern zunehmend genutzt werden, etwa zur Back-Up-Sicherung von Kommunikationsinhalten bei der Nutzung von Messengerdiensten. Weitergehende Dienstleistung im Rahmen einer Cloud bedürfen hinsichtlich der Verschlüsselung besonderer Vereinbarungen zwischen Nutzer und Anbieter. Dabei handelt es sich nicht um einen Telekommunikationsdienst, sondern um einen Telemediendienst, für den das Fernmeldegeheimnis nicht gilt. Anbieter von Clouddiensten sollten zur Gewährleistung des Datenschutzes und der Cybersicherheit im Rahmen ihrer technischen und organisatorischen Vorkehrungen gewährleisten, dass die Nutzer solcher Dienste die gespeicherten Informationen mit einer sicheren und durchgängigen Verschlüsselung schützen können. Das Recht auf Verschlüsselung ist hier eine Informationspflicht des Anbieters, da die Verschlüsslung in den Händen des jeweiligen Nutzers liegt.

4. Klarstellungen und Ergänzungen im Bereich der Aufsicht und Regelungen im Hinblick auf die Verordnung (EU) 2023/1543

Neben dem Recht auf Verschlüsselung dient der Gesetzentwurf auch der Vornahme von klarstellenden und ergänzenden Anpassungen von Bestimmungen zur Aufsicht durch BfDI und Bundesnetzagentur. Weiterhin werden Regelungen getroffen, die es vom TTDSG erfassten Adressaten von Herausgabe- und Sicherungsanordnungen von elektronischen Beweismitteln ermöglichen, ihren Pflichten nach der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren nachzukommen.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf beinhaltet eine Begriffsbestimmung der Ende-zu-Ende-Verschlüsselung, eine Ergänzung des Grundsatzes der Vertraulichkeit der Kommunikation um die zu gewährleistende Ende-zu-Ende-Verschlüsselung sowie eine Ergänzung der technischen und organisatorischen Vorkehrungen im Hinblick auf das Recht auf Ende-zu-Ende-Verschlüsselung bei der Nutzung von Clouddiensten. Weiterhin enthält der Gesetzentwurf weitestgehend klarstellende und ergänzende Anpassungen im Bereich der Aufsicht durch BNetzA und BfDI. Der Gesetzentwurf beinhaltet darüber hinaus die Rechtsgrundlangen zur Verarbeitung von Verkehrs-, Standort-, Bestands- und Nutzungsdaten zur Erfüllung der Pflichten nach der Verordnung (EU) 2023/1543.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Die Gesetzgebungszuständigkeit des Bundes ergibt sich hinsichtlich der Bestimmungen zum Telekommunikationsdatenschutz aus der ausschließlichen Zuständigkeit für das Recht der Telekommunikation (Artikel 73 Absatz 1 Nummer 7 Grundgesetz). Die Regelung des Datenschutzes für den Bereich der Telemedien folgt aus der konkurrierenden Gesetzgebung des Bundes für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 Grundgesetz).

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Es bestehen keine entgegenstehenden Vorgaben des Rechts der Europäischen Union. Die Verpflichtungen aus der Richtlinie EU/2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. EG Nr. L 241 S. 1 vom 17.09.2015) sind beachtet worden.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf enthält keine Regelungen zur Rechts- und Verwaltungsvereinfachung.

2. Nachhaltigkeitsaspekte

Regeln und Indikatoren der deutschen Nachhaltigkeitsstrategie sind nicht berührt.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

4. Erfüllungsaufwand

Es entstehen allerdings Informationspflichten zur Ende-zu-Ende-Verschlüsselung, die die betroffenen Anbieter gegenüber den Endnutzern erfüllen müssen, von denen allerdings mit Blick auf die ohnehin bereits umfangreichen und laufend aktualisierten Datenschutzinformationen kein erheblicher zusätzlicher Erfüllungsaufwand erwartet wird.

Im Übrigen wird von der Umsetzung des Rechts auf Ende-zu-Ende-Verschlüsselung ebenfalls kein nennenswerter Erfüllungsaufwand erwartet. Demgegenüber legt die Wirtschaft großen Wert auf die Gewährleistung einer sicheren Ende-zu-Ende-Verschlüsselung und sieht dies als einen Grundpfeiler des Wirtschaftsstandorts Deutschland an.

Ende-zu-Ende-Verschlüsselung ist z. B. innerhalb von Messengerdiensten Branchenstandard, wie das BKartA festgestellt hat. Die Regelung verlangt nicht zwingend, dass Dienste technische Anpassungen vornehmen müssen. Zumindest für die nicht-echtzeitbasierte Kommunikation (also Text-Messaging, E-Mail oder Dateiaustausch) ist es den Nutzern immer möglich, eine eigene und vom Anbieter unabhängige Ende-zu-Ende-Verschlüsselung einzusetzen. Daher könnte der Anbieter hier ohne jeglichen Anpassungsbedarf die Vorgaben einhalten, solange er dies nicht verhindert. Betroffene Dienste mit technischen Konfigurationen, die aktiv verhindern, dass eine wirksame Ende-zu-Ende-Verschlüsselung vorgenommen werden kann, sind nicht bekannt. Bei anderen Diensten hängt das Recht auf Ende-zu-Ende-Verschlüsselung ohnehin zunächst davon ab, dass sie technisch möglich ist, etwa im Bereich der Sprach- und Videokommunikation, insbesondere wenn mehrere Personen beteiligt sind (siehe dazu die Ausführungen unter I.).

5. Weitere Kosten

Sonstige Kosten für die Wirtschaft, für soziale Sicherungssysteme, Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Die mit einem Recht auf Ende-zu-Ende-Verschlüsselung verbundene Verbesserung des Schutzes der Vertraulichkeit der Kommunikation wirkt sich positiv auf den Schutz der Privatsphäre wie auch von Berufs- und Geschäftsgeheimnissen in der elektronischen Kommunikation aus. Der Gesetzentwurf hat keine gleichstellungspolitischen und demografischen Auswirkungen und wirkt sich auch nicht auf die Wahrung und Förderung gleichwertiger Lebensverhältnisses aus.

VII. Befristung; Evaluierung

Eine Befristung oder eine Evaluierung sind nicht vorgesehen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Telekommunikation-Telemedien-Datenschutz-Gesetzes)

Zu Nummer 1

Nummer 1 enthält die Anpassungen der Inhaltsübersicht im Hinblick auf die Einfügung neuer Paragraphen in das TTDSG.

Zu Nummer 2

Mit § 2 Absatz 2 Nummer 7 wird der Begriff der sicheren Ende-zu-Ende-Verschlüsselung bestimmt. Diese liegt vor, wenn der Kommunikationsinhalt auf dem gesamten Transportweg vom Endnutzer zum Endnutzer verschlüsselt bleibt und dazwischen nicht durch den Anbieter des Telekommunikationsdienstes oder Dritte eingesehen werden kann. Eine sichere Ende-zu-Ende-Verschlüsselung impliziert auch, dass der Schlüssel ausschließlich beim Endnutzer liegt und auch der Anbieter des Telekommunikationsdienstes diesen nicht erlangen kann. Von der Ende-zu-Ende-Verschlüsselung ist die Transportverschlüsselung oder Punkt-zu-Punkt-Verschlüsselung zu unterscheiden, bei der die Kommunikationsinhalte auf den Zwischenstationen der Übermittlung wie den Servern der Telekommunikationsanbieter unverschlüsselt sind und durch diese oder Dritte eingesehen werden können.

Mit § 2 Absatz 2 Nummer 8 wird der Begriff der Teilnehmerdaten unter Verweis auf die in Artikel 3 Nummer 9 der Verordnung (EU) 2023/1543 enthaltene Definition festgelegt. Die Begriffsbestimmung ist im TTDSG erforderlich im Hinblick auf die Befugnis zur Datenverarbeitung zum Zweck der Erfüllung von Herausgabe- und Sicherungspflichten von elektronischen Beweismitteln gemäß der Verordnung (EU) 2023/1543. Die Datenverarbeitung ist genau auf den Bereich von personenbezogenen Daten zu beschränken, der von der Europäischen Herausgabe- oder Sicherungsanordnung erfasst wird.

Zu Nummer 3

Mit § 3 Absatz 5 werden Anbieter von nummernunabhängigen interpersonellen Telekommunikationsdiensten verpflichtet, die sichere Ende-zu-Ende-Verschlüsselung durchzuführen oder gewährleisten, dass Endnutzer diese Dienste mit einer sicheren Ende-zu-Ende-Verschlüsselung nutzen können. Damit erhalten Endnutzer das Recht auf Ende-zu-Ende-Verschlüsselung ihrer Kommunikation als Teil des Schutzes der Vertraulichkeit der Kommunikation und des Fernmeldegeheimnisses. Die Ende-zu-Ende-Verschlüsselung schützt die zu übertragenden Datenpakete hinsichtlich der Vertraulichkeit dahingehend, dass die Kommunikationsinhalte über den gesamten Übertragungsweg unlesbar sind. Dies kann nur durch eine sichere Ende-zu-Ende-Verschlüsselung gewährleistet werden, bei der die Daten beim Absenden verschlüsselt und erst beim Empfänger wieder entschlüsselt werden.

Die Regelung enthält keine unmittelbare Verpflichtung der betroffenen Anbieter, die Ende-zu-Ende-Verschlüsselung selbst zu veranlassen. Sie müssen dies aber ermöglichen und dürfen keine technischen oder organisatorischen Maßnahmen ergreifen, die den Einsatz von üblicherweise verwendeten Verfahren zur durchgängigen und sicheren Ende-zu-Ende-Verschlüsselung seitens der Endnutzer erschweren oder verhindern. Dies spiegelt die derzeitige Praxis der Anbieter wieder, die die Ende-zu-Ende-Verschlüsselung teilweise selbst vornehmen oder die Aktivierung dem Endnutzer überlassen. Diese Praxis wird durch das Recht auf Verschlüsselung nicht berührt.

Das Recht auf Ende-zu-Ende-Verschlüsselung wird ergänzt durch die Pflicht, die Endnutzer entsprechend zu informieren. Die Informationspflicht wirkt Transparenzmängeln bei Verbraucherinnen und Verbrauchern entgegen, die das BKartA in seinem Abschlussbericht zur Sektoruntersuchung zu Messenger- und Videodiensten erkannt hat. Ist aus technischen Gründen eine Ende-zu-Ende-Verschlüsselung nicht möglich, informiert der Anbieter des

Telekommunikationsdienstes den Endnutzer über die technischen Gründe, die einer Ende-zu-Ende-Verschlüsselung entgegenstehen.

Ein Stand der Technik von Verschlüsselungsverfahren wird nicht bestimmt. Die derzeit verwendeten Techniken nutzen ein asymmetrisches Verschlüsselungsverfahren, bei dem ein Schlüsselpaar zum Einsatz kommt, das aus einem öffentlichen und einem privaten Schlüssel besteht. Mit dem öffentlichen Schlüssel wird die Kommunikation durch den absendenden Endnutzer verschlüsselt. Diese kann dann nur durch den privaten Schlüssel des empfangenden Endnutzers wieder entschlüsselt werden.

Zu Nummer 4

Nummer 4 enthält eine notwendige Regelung, die es gewerblich angebotenen Telekommunikationsdiensten rechtlich ermöglicht, Teilnehmerdaten (siehe zu Nummer 2) Verkehrsdaten und Standortdaten zu verarbeiten, um ihren Pflichten nach der Verordnung (EU) 2023/1543 nachzukommen. Die Verordnung regelt im Rahmen von Strafverfahren die Herausgabe oder Sicherung von elektronischen Beweismitteln durch betroffene Diensteanbieter auf der Grundlage von sogenannten „Europäischen Herausgabeanordnungen“ oder „Europäischen Sicherungsanordnungen“ die von zuständigen Behörden in einem Mitgliedstaat erlassen werden. Diese können damit von einem Diensteanbieter, der in der Union Dienste anbietet und in einem anderen Mitgliedstaat zum Empfang von Anordnungen einen Vertreter bestellt bzw. eine Niederlassung benannt hat, verlangen, elektronische Beweismittel herauszugeben oder zu sichern, unabhängig davon, wo sich die Daten befinden.

Die Verordnung (EU) 2023/1543 enthält zwar die Verpflichtung der Adressaten, einer solchen Herausgabe- oder Sicherungsanordnung nachzukommen, jedoch keine Regelung, die den Adressaten auch befugt, personenbezogene Daten zu diesem Zweck zu verarbeiten. Das ist jedoch in Deutschland im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung und zur Wahrung des Telekommunikationsgeheimnisses erforderlich. Der Gesetzgeber muss nach dem Bild einer Doppeltür sowohl für die Übermittlung der personenbezogenen Daten durch die Telekommunikationsanbieter als auch für den Abruf dieser Daten durch die Behörden jeweils verhältnismäßige Rechtsgrundlagen schaffen. Übermittlungs- und Abrufregelungen müssen die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen (vgl. BVerfG Beschluss vom 27. Mai 2020 - 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II). Das TTDSG enthält bisher keine Regelung, die betroffene Diensteanbieter zur Verarbeitung von Verkehrs- oder Standortdaten zum Zwecke der Europäischen Herausgabe- oder Sicherungsanordnung befugt. Das TTDSG stünde daher ohne eine solche Regelung der Herausgabe und Sicherung von elektronischen Beweismitteln, bei denen es sich um die Verarbeitung von Verkehrs- oder Standortdaten handelt, ohne eine solche Regelung entgegen.

Gemäß Artikel 3 Nummer 8 dieser Verordnung sind elektronische Beweismittel Teilnehmerdaten, Verkehrsdaten oder Inhaltsdaten, die zum Zeitpunkt des Erhalts einer Bescheinigung über eine Europäische Herausgabeanordnung oder einer Bescheinigung über eine Europäische Sicherungsanordnung von einem Diensteanbieter oder in seinem Auftrag gespeichert werden. Verkehrs- und Inhaltsdaten nach der Verordnung (EU) 2023/1543 (Artikel 3 Nummer 11 und 12) entsprechen den Verkehrs- und Standortdaten des TTDSG. Dabei sind Verkehrsdaten nach dem TTDSG sowohl die Inhaltsdaten wie auch die Metadaten wie Ursprung und Ziel einer Nachricht, Daten über den Standort des Geräts, Datum, Uhrzeit, Dauer, Größe, Route, Format, verwendetes Protokoll und Art der Kompression. Adressaten einer Europäischen Herausgabeanordnung und Europäischen Sicherungsanordnung sind Diensteanbieter, worunter elektronische Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972 fallen (Artikel 3 Nummer 3 Buchstabe a der Verordnung (EU) 2023/1543). Das sind in der Regel gegen Entgelt, d. h. gewerblich erbrachte Internetzugangsdienste, interpersonelle Kommunikationsdienste (sowohl nummerngebundene wie auch nummernunabhängige) und Dienste, die ganz oder überwiegend in der

Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden. Rein geschäftsmäßig erbrachte Telekommunikationsdienste, die nicht gewerblich erbracht werden, d. h. ohne Teil einer wirtschaftlichen Gegenleistung zu sein wie bei der Bereitstellung von Telekommunikation innerhalb von Unternehmen oder sonstigen Organisationen im Rahmen von Arbeits- oder Dienstverhältnissen, unterliegen keiner Herausgabe- oder Sicherungsanordnung und benötigen daher keine Befugnis zur Verarbeitung von Verkehrs- oder Standortdaten.

Zu Nummer 5

In § 19 Absatz 6 wird eine Informationspflicht hinsichtlich der Möglichkeiten einer sicheren und durchgehenden Verschlüsselung der bereitgestellten Informationen bei der Nutzung von Cloud-Speichern eingeführt. Clouddienste sind Telemedien, die darin bestehen, von einem Nutzer bereitgestellte Informationen für diesen zu speichern. Die Nutzung von Clouddiensten zur Speicherung von privaten wie auch von Unternehmensdaten ist immer stärker verbreitet. Die sichere und durchgehende Verschlüsselung von Informationen auf Cloudspeichern ist technisch möglich und dient der Datensicherheit was den Schutz vor Cyberangriffen im Allgemeinen und den Schutz der personenbezogenen Daten im Besonderen anbelangt. Die meisten Unternehmen nutzen inzwischen Clouddienste zur Verlagerung von Speicherplatz, Rechenkapazität oder Software-Anwendungen auf externe Server. Zudem nutzt ein immer größerer Anteil von Bürgern und Bürgerinnen Clouddienste, etwa zum Backup-Speichern von Nachrichten bei Messengerdiensten. Eine durchgehende und sichere Verschlüsselung von Informationen in der Cloud, die gewährleistet, dass diese Informationen nur von dem sie bereitstellenden Nutzer gelesen werden können, ist damit ebenso wichtig wie im Rahmen der Nutzung von nummernunabhängigen interpersonellen Telekommunikationsdiensten. Daher sollten Anbieter von Cloudspeichern darüber informieren.

Zu Nummer 6

Wie in Nummer 4 bedarf es auch für die von der Verordnung (EU) 2023/1543 betroffenen Telemedienanbieter einer besonderen Rechtsgrundlage zur Verarbeitung von Teilnehmer- und Nutzungsdaten, ohne die eine an diese Anbieter gerichtete Europäische Herausgabe- oder Sicherungsanordnung ins Leere laufen würde. Das TTDSG hat Auskunftserteilung über Bestands- und Nutzungsdaten in den §§ 21-24 in engen Grenzen geregelt. Befugnisse zur Datenverarbeitung zum Zweck der Sicherung und Übermittlung von elektronischen Beweismitteln auf der Grundlage einer Europäischen Herausgabe- oder Sicherungsanordnung sind darin nicht erhalten. Der neue § 24a schließt diese Lücke. Dabei betrifft die Verordnung (EU) 2023/1543 nicht alle Telemedienanbieter (in der Verordnung Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535), sondern nur die gewerblichen Anbieter von Telemedien die es ihren Nutzern ermöglichen, miteinander zu kommunizieren oder Daten zu speichern oder auf sonstige Weise zu verarbeiten, sofern die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist. Entsprechend ist auch die erforderliche Befugnis zur Datenverarbeitung auf diese Anbieter zu beschränken. Zu den von Europäischen Herausgabe- oder Sicherungsanordnungen betroffenen Telemedienanbietern gehören beispielsweise Online-Marktplätze, die es Verbrauchern und Unternehmen ermöglichen, miteinander zu kommunizieren, und andere Hosting-Dienste, einschließlich Cloud-Computing-Diensten, sowie Plattformen für Online-Spiele und Online-Glücksspiele. Nicht darunter fallen Telemedien, die es ihren Nutzern nicht ermöglichen, miteinander zu kommunizieren, sondern lediglich eine Kommunikation mit dem Diensteanbieter bietet. Ebenfalls nicht darunter fallen Telemedien, die es ihren Nutzern nicht ermöglichen, Daten zu speichern oder anderweitig zu verarbeiten, oder wenn die Datenspeicherung kein bestimmender, also kein wesentlicher Bestandteil der für den Nutzer erbrachten Dienstleistung ist, wie im Fall online erbrachter Rechts-, Architektur-, Ingenieur- und Buchführungsleistungen (Erwägungsgrund 27 der Verordnung (EU) 2023/1543). Die Verordnung betrifft mit auch weitere Anbieter (Anbieter von Internetdomänennamen- und IP-Nummerierungsdiensten wie Diensten der IP-

Adressenzuweisung und der Domänennamen-Registrierung, Anbieter von Domänennamen-Registrierungsstellendienste und Anbieter von mit Domänennamen verbundenen Datenschutz- und Proxy-Diensten), die neben den bestimmten Diensten der Informationsgesellschaft genannt werden, bei denen es sich aber gleichwohl ebenfalls um Telemedien handelt. Auch für diese Anbieter wird die erforderliche Befugnis zur Datenverarbeitung in § 24a geregelt.

Zu Nummer 7

Mit den Änderungen in § 28 erfolgt eine Bußgeldbewehrung gegen die Informationspflicht über die Ende-zu-Ende-Verschlüsselung gemäß § 3 Absatz 5, die durch die Bundesnetzagentur beaufsichtigt wird. Weiterhin erfolgt eine Bußgeldbewehrung, wenn Clouddienste die Anforderungen des § 19 Absatz 6 nicht erfüllen.

Zu Nummer 8

Zu Buchstabe a

Die Neufassung des § 29 Absatz 1 dient der Klarstellung der Aufsichtszuständigkeit des oder der BfDI. Diese® ist zuständig für die Einhaltung der gesetzlichen Anforderungen an die Verarbeitung von personenbezogenen Daten durch Telekommunikationsunternehmen, wie sie sich aus der DSGVO und hinsichtlich der erlaubten Verarbeitung von Verkehrs- und Standortdaten speziell aus dem TTDSG ergeben. Die Zuständigkeit des oder der BfDI im Hinblick auf die Einhaltung der allgemeinen Datenschutzbestimmungen der DSGVO ist in § 9 Absatz 1 Bundesdatenschutzgesetz geregelt und bedarf hier keiner Wiederholung. Die Aufsicht des oder der BfDI bezieht sich auf die im TTDSG geregelten speziellen Erlaubnistatbestände zur Verarbeitung von Verkehrsdaten in den §§ 9, 10, 12 und zur Verarbeitung von Standortdaten in § 13. Die Klarstellung deckt sich mit der Regelung zur Bußgeldzuständigkeit in § 28 TTDSG und dient der genaueren Abstimmung mit der Aufsichtszuständigkeit der BNetzA, die gemäß § 30 die zuständige Aufsichtsbehörde für alle anderen Bestimmungen des Teils 2 des TTDSG ist.

Zu Buchstabe b

Die Ergänzung in Absatz 2 weist dem oder der BfDI auch die Aufsicht im Hinblick darauf zu, das Postdienste auf Endeinrichtungen des Endnutzers zugreifen. Postdienste unterliegen wie Telekommunikationsdienste der Aufsicht durch den oder die BfDI.

Zu Buchstabe c

Die Ergänzung in Absatz 3 zielt darauf ab, klarzustellen, dass der oder die BfDI im Rahmen der Aufgabenwahrnehmung keine geringeren Befugnisse hat als die BNetzA nach § 30.

Zu Nummer 9

Die Ergänzung von § 30 um einen neuen Absatz 6 dient der Schließung einer Gesetzeslücke bei der Durchsetzung des Verbotes nach § 8. Im Rahmen des Onlinehandels mit nach § 8 verbotenen Telekommunikationsanlagen sind Betreiber von dazu genutzten Online-Plattformen derzeit nicht befugt, der Bundesnetzagentur Auskunft über personenbezogene Daten von Verkäufern und Käufern zu erteilen, weil dazu keine Rechtspflicht besteht und dementsprechend auch kein Recht nach Artikel 6 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), personenbezogene Daten zu diesem Zweck zu verarbeiten. Die Bundesnetzagentur hat daher derzeit keine Möglichkeit, Besitzer verbotener Telekommunikationsanlagen zu ermitteln und gegen den Besitz vorzugehen, wenn die betreffenden Telekommunikationsanlagen über Online-Verkaufsplattformen erworben wurden.

Zu Artikel 2 (Inkrafttreten, Außerkrafttreten)

Artikel 2 bestimmt das Inkrafttreten auf den 1. April 2025.