DIGITALEUROPE

20. NOVEMBER 2020

Stellungnahme zum deutschen Gesetzentwurf zur Umsetzung des EECC

Zusammenfassung

DIGITALEUROPE hat die vorgeschlagenen Änderungen des deutschen Telekommunikationsgesetzes (das „TKG“)[1] gemäß dem von der deutschen Regierung veröffentlichten Entwurf (der „Gesetzentwurf“)[2], der den Europäischen Kodex für elektronische Kommunikation (European Electronic Communications Code[3], „EECC“) umsetzen soll, untersucht und möchte die folgenden Anmerkungen mitteilen.

Zunächst einmal möchte DIGITALEUROPE anmerken, dass der EECC – als erste Richtlinie, die OTT-Kommunikationsdienste der regulatorischen Aufsicht unterstellt – für diese bewusst nur leichtere Verpflichtungen aufstellt und damit einen abgestuften Ansatz verfolgt. Insbesondere unterscheiden sich nummernunabhängige interpersonelle Kommunikationsdienste grundlegend von herkömmlichen Diensten. Nummernunabhängige interpersonelle Kommunikationsdienste sind in der Regel kostenlose oder kostengünstige Dienstleistungen, die durch niedrige Eintrittsbarrieren und zahlreiche konkurrierende Anbieter gekennzeichnet sind. Die meisten Anbieter dieser Dienste haben nur wenig oder gar keine Kontrolle über private und geschäftliche Internet-Zugangsdienste und Netze, die zur Übertragung ihrer Dienste verwendet werden. Der EECC erkennt diese Unterschiede an und legt für nummernunabhängige interpersonelle Kommunikationsdienste bewusst

[1] Telekommunikationsgesetz vom 22. Juni 2004, zuletzt geändert am 6. Juni 2020.

[2] Gesetzentwurf für die Umsetzung der Richtlinie (EG) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Etablierung des Europäischen Kodex für elektronische Kommunikation (Neufassung) und für die Modernisierung des Telekommunikationsgesetzes (TKModG) vom 2. November 2020.

[3] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Etablierung des Europäischen Kodex für elektronische Kommunikation (Neufassung).

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

unterschiedliche und deutlich weniger belastende Anforderungen im Vergleich zu anderen Arten von elektronischen Kommunikationsdiensten (ECS) fest[4].

DIGITALEUROPE ist besorgt, dass einige Bestimmungen des Gesetzentwurfs diesen graduellen, kontextabhängigen Ansatz nicht widerspiegeln und auch über das im EECC vorgesehene Maß an Harmonisierung hinausgehen. DIGITALEUROPE möchte die Bedeutung einer Harmonisierung mit dem Ziel der Realisierung und Stärkung des digitalen Binnenmarktes unterstreichen. Wir sind der Ansicht, dass die Bestimmungen im Gesetzentwurf in einer Reihe von Bereichen zu unverhältnismäßigen Verpflichtungen führen würden, die dem freien Verkehr von Dienstleistungen entgegenstehen und in anderen Bereichen die nationalen Befugnisse im Rahmen des EECC-Rahmenwerks übersteigen würden. Nachfolgend erklären wir diese Bedenken ausführlicher, betonen jedoch Folgendes als besonders wichtig:

- Die Definition in § 3 Nr. 3 TKG („*Anschlusskennung*“) kann in Verbindung mit den Verpflichtungen in Teil 10 als eine Verpflichtung für Anbieter von nummernunabhängigen interpersonelle Kommunikationsdiensten zur Erhebung und Erzeugung von Nutzerdaten interpretiert werden, wobei unklar ist, welche Daten erfasst werden sollen/müssen, insbesondere in Verbindung mit §169 Absatz 3 TKG. Es ist beispielsweise unklar, ob Kontonamen oder *nicknames* darunter fallen, die als Nutzeridentifikation für nummernunabhängige interpersonelle Kommunikationsdienste dienen. In diesem kritischen Bereich, in dem es starke politische Argumente sowohl für als auch gegen die Datenerhebung gibt, sollte der Gesetzgeber besonders klar sein, was die genauen Anforderungen an Anbieter betrifft.
- §169 TKG: Die Umsetzung des EECC in nationales Recht bot dem Gesetzgeber die Möglichkeit, die gesamte Regelung zur öffentlichen Sicherheit neu zu gestalten, die bereits mehrfach höchstrichterlich kritisiert und teilweise für unwirksam erklärt wurde. Stattdessen wurde der Umfang einiger Maßnahmen ohne Berücksichtigung gerichtlicher Vorgaben erweitert. Die im Juli 2020 veröffentlichte Entscheidung des Bundesverfassungsgerichts hat nicht nur Einfluss auf § 171 des Gesetzentwurfs, auch §§ 169 und 170 sind betroffen und sollten zurückgezogen und durch ein rechtskonformes und transparenteres Regelwerk ersetzt werden.

[4] EG 44: „Im Gegensatz zu anderen Kategorien elektronischer Kommunikationsnetze und -dienste im Sinne dieser Richtlinie profitieren nummernunabhängige interpersonelle Kommunikationsdienste nicht von der Nutzung öffentlicher Nummerierungsressourcen und sind nicht am öffentlich gesicherten interoperablen Ökosystem beteiligt. Daher ist es nicht angezeigt, diese Dienstarten der Regelung für Allgemeingenehmigungen zu unterwerfen“.

Inhaltsverzeichnis

- Zusammenfassung 1
- Inhaltsverzeichnis 3
- Definitionen (Art. 2 EECC / § 3 Gesetzentwurf) 4
- Meldung an die Bundesnetzagentur (Art. 12 EECC / § 5 Gesetzentwurf)..... 5
- Auskunftsverlangen (Art. 20 EECC)..... 5
- Sicherheit von Netzen und Diensten (Art. 40 EECC / § 162 Gesetzentwurf)..... 6
- Verhandlungspflicht (Art. 60 EECC / §18 Gesetzentwurf)..... 9
- Endnutzerrechte (Art. 102 ff. EECC / § 50 Gesetzentwurf)..... 9
- Notruf (Art. 109 EECC / § 161 Gesetzentwurf) 11
- Daten für Auskunftsersuchen / automatisierte Auskunftsverfahren (§§ 169 und 170 Gesetzentwurf) 13
- Manuelles Auskunftsverfahren (§ 171 Gesetzentwurf)..... 16

Definitionen (Art. 2 EECC / § 3 Gesetzentwurf)

DIGITALEUROPE begrüßt, dass die meisten Definitionen des Gesetzentwurfs den EECC-Definitionen sehr nahe kommen oder ihnen entsprechen. Im Einklang mit dem Ansatz in Erwägungsgrund (18) EECC[5] befürwortet DIGITALEUROPE insbesondere die wichtige Klärung bezüglich der Nutzung von Nummern im Kontext von § 3 Nr. 34 in der Begründung zum Gesetzentwurf, dass die Zuweisung von Nummern der Bereitstellung einer Ende-zu-Ende-Konnektivität dient und dass der Zweck der Ermöglichung der Kommunikation mit Nummern darin besteht, andere Endnutzer, denen diese Nummern zugewiesen wurden, über das öffentlich gesicherte interoperable Ökosystem zu erreichen.

Es gibt jedoch einen Aspekt der Definitionen, bei dem eine weitergehende Klärung hilfreich wäre.

- § 3 Nr. 3 („*Anschlusskennung*"), eine Bestimmung, die den Umfang der kritischen Verpflichtung von nummernunabhängigen interpersonellen Kommunikationsdiensten zur Erhebung von Nutzerdaten nach § 169 bestimmt, lässt zu viel Raum für Interpretationen hinsichtlich der Frage, welche Daten davon erfasst werden. Wie nachstehend erläutert, ist DIGITALEUROPE der Ansicht, dass die Erhebung von Daten nach § 169 als solche unverhältnismäßig und für nummernunabhängige interpersonelle Kommunikationsdienste unzulässig ist. Dennoch fordern wir den deutschen Gesetzgeber auf, den Geltungsbereich der Definition klarzustellen, damit die Anforderungen eindeutig sind, falls diese Verpflichtung im Gesetzentwurf bleiben sollte. Die Begründung zum Gesetzentwurf ist an dieser Stelle nur wenig hilfreich; sie besagt nur, dass Telefonnummern eine Untergruppe von Anschlusskennungen sind, die wiederum eine Untergruppe der „*Kennungen*" sind. Es existiert jedoch keine rechtliche Definition von „*Kennungen*" im Gesetzentwurf. Daher schaffen die Verpflichtungen Rechtsunsicherheit. Zum Beispiel erheben nummernunabhängige interpersonelle Kommunikationsdienste in der Regel keine Namen von Nutzern; sofern sie erhoben werden, können Online-Nutzernamen grundsätzlich vom Nutzer frei geändert werden. Dies unterscheidet sie von den Namen, die von herkömmlichen nummerngebundenen Diensten für Abrechnungszwecke erhoben werden, und die mit höherer Wahrscheinlichkeit feststehend und eindeutig sind. Es ist jedoch nicht hinreichend klar, dass informelle,

[5] In Erwägungsgrund 18 heißt es: „Die bloße Nutzung einer Nummer als Kennung sollte nicht mit der Nutzung einer Nummer zur Herstellung einer Verbindung mit öffentlich zugeteilten Nummern gleichgesetzt und daher für sich allein nicht als ausreichend betrachtet werden, um einen Dienst als nummerngebundenen interpersonellen Kommunikationsdienst zu bezeichnen".

temporäre Nutzernamen nicht vom Geltungsbereich der § 3 Nr. 3 und § 169 erfasst werden würden.

Meldung an die Bundesnetzagentur (Art. 12 EECC / § 5 Gesetzentwurf)

Obwohl der Gesetzentwurf den Art. 12 des EECC korrekt widerspiegelt und nur von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich verfügbarer nummernbasierter interpersoneller Kommunikationsdienste eine Meldung verlangt, weist der Entwurf in einem Kommentar auch darauf hin, dass eine Erweiterung des Kreises der verpflichteten Anbieter in Betracht gezogen werden könnte. DIGITALEUROPE ist der Meinung, dass eine solche Erweiterung gegen Art. 12 EECC verstoßen würde und fordert, dass der aktuelle Text im weiteren Gesetzgebungsverfahren beibehalten wird.

DIGITALEUROPE stellt fest, dass der Gesetzentwurf verlangt, Änderungen sowie die Einstellung der Geschäftstätigkeit zu melden. Genau genommen geht dies über Art. 12 (4) EECC hinaus, der eine vollständige Liste der Arten von Informationen enthält, die von den Unternehmen, die den entsprechenden allgemeinen Meldepflichten unterliegen, gefordert werden können. Art. 12 (4) EECC besagt ausdrücklich, dass die Mitgliedstaaten keine zusätzlichen oder separaten Meldepflichten auferlegen dürfen. DIGITALEUROPE ersucht darum, dass § 5 des Gesetzentwurfs an Art. 12 (4) EECC angepasst wird.

Wir weisen auch darauf hin, dass die Bundesnetzagentur (BNetzA) beauftragt wurde, ein Muster für die Meldungen zu entwickeln. In Anbetracht der Tatsache, dass GEREK Leitlinien[6] für ein Meldemuster entwickelt hat, könnte das deutsche Gesetz hierauf Bezug nehmen und diesen so weit wie möglich folgen. Dies wird dazu beitragen, den Binnenmarkt zu fördern und die Belastungen für grenzüberschreitende Anbieter zu reduzieren.

Auskunftsverlangen (Art. 20 EECC)

Art. 20 EECC legt fest, dass alle Auskunftsverlangen, die an Anbieter von elektronischen Kommunikationsdiensten und elektronischen Kommunikationsnetzen (ECN) gerichtet werden, im angemessenen Verhältnis zur Wahrnehmung der Aufgabe der nationalen Regulierungsbehörde stehen und begründet sein müssen. Art. 20 EECC wurde im Gesetzentwurf in einer Vielzahl von Bestimmungen umgesetzt, einschließlich §§ 4, 196, 200 und 201. Diese

[6] Verfügbar unter https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/8911-berec-guidelines-for-the-notification-template-pursuant-to-article-12-paragraph-4-of-directive-20181972-of-the-european-parliament-and-of-the-council.

Bestimmungen sehen jedoch nicht vor, dass Informationsanforderungen im Verhältnis zur Wahrnehmung der Aufgabe stehen müssen. Wenngleich DIGITALEUROPE darauf vertraut, dass die Auskunftsverlangen der deutschen Behörden nicht über das hinausgehen, was für die Wahrnehmung der spezifischen Aufgabe im Interesse der Öffentlichkeit erforderlich ist, würden wir eine Klarstellung dieser Anforderung gemäß Art. 20 (1) (UAbs 5) EECC begrüßen.

Sicherheit von Netzen und Diensten (Art. 40 EECC / § 162 Gesetzentwurf)

Art. 40 EECC verlangt von den Mitgliedstaaten, sicherzustellen, dass Anbieter von *öffentlichen* elektronischen Kommunikationsnetzen (ECN) oder von öffentlich zugänglichen ECS angemessene und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihrer Netze und Dienste zu gewährleisten.

§ 162 Abs. 1 des Gesetzentwurfs jedoch weitet diese Verpflichtung scheinbar auf *private* Dienste aus, indem er „jeden, der Telekommunikationsdienstleistungen erbringt“ anspricht. Während sich die nachfolgenden Unterabsätze von § 162 richtigerweise nur auf öffentliche Netze und Dienste konzentrieren, integrieren sie nicht ausdrücklich den vom EECC geforderten abgestuften Ansatz, nämlich eine differenzierte, angemessene und verhältnismäßige Regulierung von nummernbasierten und nummernunabhängigen interpersonellen Kommunikationsdiensten[7].

Die Notwendigkeit eines spezifischen Sicherheitssystems für OTT-Anbieter wird ebenfalls von ENISA und der Expertengruppe gemäß Artikel 13a erkannt. Insbesondere in der kürzlich von der Expertengruppe nach Artikel 13a durchgeführten Konsultation zur Festlegung der technischen Leitlinie zu Sicherheitsmaßnahmen nach dem EECC (die die bestehende technische Leitlinie[8] ersetzen soll) merkt die Expertengruppe in Abschnitt 5.3 an, dass „dies in der Praxis bedeutet, dass abhängig von den Einstellungen, der Art des Netzes oder der angebotenen Dienste, der betroffenen Assets etc. einige der

[7] Erwägungsgrund 95: „Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Wenn dies auf der Grundlage der tatsächlichen Bewertung der bestehenden Sicherheitsrisiken gerechtfertigt ist, sollten die Maßnahmen von Anbietern nummernunabhängiger interpersoneller Kommunikationsdienste daher weniger strikt sein. Derselbe Ansatz sollte sinngemäß auch für interpersonelle Kommunikationsdienste gelten, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben“.

[8] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Sicherheitsmaßnahmen in dieser Leitlinie möglicherweise nicht vollständig auf OTT-Anbieter anwendbar sind. Bei der Bewertung, ob die Anbieter die Anforderungen des Artikel 40 erfüllen, sollten die zuständigen Behörden die Art des angebotenen Netzes oder Dienstes, die betroffenen Assets, die Bedrohungen und die daraus resultierenden Risiken für dieses Netz und diesen Dienst berücksichtigen“.

DIGITALEUROPE betont, dass es von entscheidender Bedeutung ist, dass die deutschen Behörden dem ausgewogenen Verhältnis im EECC Rechnung tragen, wenn sie das Gesetz auf nummernunabhängige interpersonelle Kommunikationsdienste anwenden. Tatsächlich heißt es in § 162 (5) des Gesetzentwurfs:

> „Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. § 62 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend“.

Im Einklang mit dieser Bestimmung und dem EECC muss im Rahmen der Sicherheitsanforderungen berücksichtigt werden, dass nummernunabhängige interpersonelle Kommunikationsdienste grundsätzlich keine Kontrolle über die Netze ausüben, die die Signale übertragen.

Andere Anforderungen, wie die Ernennung einer Kontaktperson in der EU und eines Sicherheitsbeauftragten sowie die Einrichtung und regelmäßige Einreichung von Sicherheitskonzepten bei der Regulierungsbehörde, die in § 163 des Gesetzentwurfs vorgesehen sind, sollten ebenfalls nicht in der gleichen Weise für nummernunabhängige interpersonelle Kommunikationsdienste und andere netzunabhängige Dienste gelten, wie sie für netzbasierte Dienste gelten. Auch hier wird der unterschiedliche regulatorische Ansatz des EECC gegenüber Anbietern von nummernunabhängigen interpersonellen Kommunikationsdiensten im Vergleich zu nummernbasierten, wie er in Erwägungsgrund 95 wiedergegeben wird, in §§ 162 und 163 nicht berücksichtigt.

Ein neuer Blick darauf, wie die Sicherheitsverpflichtungen sinnvoll auf nummernunabhängige interpersonelle Kommunikationsdienste und netzunabhängige nummernbasierte Anbieter angewendet werden können, ist unserer Ansicht nach ebenfalls erforderlich, da OTT-Betreiber im Allgemeinen in einem grenzüberschreitenden Modus arbeiten. Folglich besteht bei einer traditionellen und lokalisierten Herangehensweise an Artikel 40 EECC die Gefahr, dass diese Anbieter mit sich überschneidenden und möglicherweise widersprüchlichen Anforderungen konfrontiert werden, die sie im Wesentlichen nicht erfüllen können, und dies würde auch nicht zu einer Erhöhung des allgemeinen Sicherheitsniveau führen. Außerdem hat auch ENISA insbesondere

in ihrem Bericht *Security Supervision under the EECC*[9] gefordert, dass der bestehende Rechtsrahmen in Bezug auf die zu ergreifenden Sicherheitsmaßnahmen aktualisiert werden muss und dass idealerweise unter Berücksichtigung der Spezifität der OTT-Kommunikationsdienste ein gemeinsames Modell entwickelt werden sollte.

Kritische Komponenten werden in § 162 Abs. 3 des Gesetzentwurfs behandelt und es wird auf die Definition solcher Komponenten in § 2 Nr. 13 des BSI-Gesetzes verwiesen. Dieses Gesetz befindet sich jedoch in einer frühen Phase, da lediglich ein Entwurf vom 7. Mai 2020 veröffentlicht wurde und das Gesetzgebungsverfahren ins Stocken geraten ist. DIGITALEUROPE behält sich Anmerkungen zu dieser Definition für die zukünftige Konsultation des BSI-Gesetzes vor. Wir verstehen jedoch, dass Einzelheiten der Bezeichnung von Komponenten als „kritisch“ im Katalog der Sicherheitsanforderungen gemäß § 164 (1) Nr. 2 des Gesetzentwurfs näher angesprochen werden können. DIGITALEUROPE schlägt vor, dass der Katalog gemäß § 164, einschließlich der Bestimmung kritischer Komponenten, in Absprache mit den betroffenen Anbietern und Betreibern erstellt werden sollte, und ihnen nicht nur die Möglichkeit zur Abgabe von Stellungnahmen eingeräumt werden sollte.

In Bezug auf die in § 166 des Gesetzentwurfs vorgesehenen Verpflichtungen zur Meldung von Störungen möchten wir die allgemeine Bemerkung machen, dass die gegenwärtige Umsetzung der gemäß Artikel 40 EECC vorgesehenen Verpflichtung, Sicherheitsvorfälle mit beträchtlichen Auswirkungen zu melden, für nummernunabhängige interpersonelle Kommunikationsdiensten und netzunabhängige nummernbasierte Kommunikationsdienste aufgrund des oben genannten grenzüberschreitenden Charakters von OTT-Diensten ungeeignet ist. Störungen des Dienstes, die globale OTT-Dienste betreffen, werden normalerweise nicht lokalisiert. Im Gegensatz zu den herkömmlichen Telekommunikationsnetzen und -diensten, bei denen Störungen aufgrund des Ausfalls einer bestimmten Netzkomponente, die einen bestimmten Bereich betrifft, auftreten können, können Störungen von Diensten, die auf der Basis von Internet-Zugangsdiensten bereitgestellt werden, zahlreiche Länder und Regionen umfassen und daher möglicherweise nicht eindeutig auf die eine oder andere Region zurückgeführt werden. Anstatt ein System aufzubauen, das von Dienstleistern verlangt, selbständig eine einzelne Störung anhand von bis zu 27 Kriterienkatalogen zu bewerten und dann diese gleiche Störung bis zu 27 Mal zu melden (und möglicherweise an mehrere nationale Stellen als „zuständige Behörden“ nach bis zu 27 verschiedenen Fristen) fordern wir die zuständige Behörde nachdrücklich auf, mit dem GEREK und der ENISA zusammenzuarbeiten, um ein europaweites Meldeverfahren aufzubauen,

[9] https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc/.

welches die Meldung vereinfacht und gleichzeitig die Endnutzer in ganz Europa angemessen schützt.

Verhandlungspflicht (Art. 60 EECC / §18 Gesetzentwurf)

Gemäß Art. 60 EECC sind Betreiber von ECN berechtigt und auf Antrag von hierzu gemäß Art. 15 EECC befugten Unternehmen verpflichtet, miteinander über die Zusammenschaltung zwecks Erbringung öffentlich zugänglicher elektronischer Kommunikationsdienste zu verhandeln, um die unionsweite Bereitstellung von Diensten sowie deren Interoperabilität zu gewährleisten.

§ 18 Abs. 1 des Gesetzentwurfs erstreckt diese Verpflichtung indes auf alle „Unternehmen“. Sie sind berechtigt und auf Anfrage verpflichtet, über ein Angebot von Zugang und Zusammenschaltung zu verhandeln, um die Kommunikation der Nutzer und ihre Interoperabilität im gesamten Gebiet der Europäischen Union zu gewährleisten. DIGITALEUROPE stellt fest, dass das europäische Recht in Art. 60 EECC eindeutig darauf abzielt, nur Netzbetreiber zu Verhandlungen über die Zusammenschaltung zwecks Interoperabilität zu zwingen. Andere Anbieter, insbesondere nummernunabhängige interpersonelle Kommunikationsdienste und sonstige Anbieter, die die Infrastruktur von Drittanbietern nutzen, können nicht verpflichtet werden, die Interoperabilität mit anderen Anbietern außerhalb des Umfangs und der Voraussetzungen von Art. 61 EECC zu gewährleisten, was durch § 19 Abs. 2 Nr. 1-4 des Gesetzentwurfs richtigerweise umgesetzt wird. Die in § 18 Abs. 1 vorgeschlagene Verpflichtung ist daher zu weit gefasst und führt folglich zu Verwirrung im Hinblick auf § 19. Wir fordern den Gesetzgeber dringend auf, den Geltungsbereich von § 18 im Einklang mit Artikel 60 EECC eindeutig auf öffentliche ECN-Anbieter zu beschränken.

Endnutzerrechte (Art. 102 ff. EECC / § 50 Gesetzentwurf)

DIGITALEUROPE stellt fest, dass § 50 des Gesetzentwurfs in sich widersprüchlich und unstimmig bzw. unübersichtlich ist; es ist anzunehmen, dass er dazu bestimmt ist, die Artikel 102, 103, 104 und Teile von Art. 107 des EECC zu implementieren.

§ 50 des Gesetzentwurfs ist scheinbar als teilweise Umsetzung von Art. 103 Abs. 1 EECC gemeint, der Anbieter verpflichtet, soweit ihre Dienstleistungen den Geschäftsbedingungen unterliegen, die in Anhang IX des EECC aufgeführten Informationen (Beschreibung der Dienste, Kontaktdaten,

Standardvertragsbedingungen, Tarife, Zugangsfunktionen usw.) zu veröffentlichen oder an Aufsichtsbehörden weiterzugeben.

Jedoch geht § 50 des Gesetzentwurfs über die Bestimmungen von Art. 103 Abs. 1 EECC hinaus und beabsichtigt scheinbar, Elemente anderer EECC-Artikel zu integrieren, ohne jedoch den Geltungsbereich und die Voraussetzungen all dieser Bestimmungen zu berücksichtigen. Wir haben insbesondere die folgenden Abweichungen vom EECC-Rechtsrahmen festgestellt:

- Art. 103 Abs. 1 EECC verpflichtet Anbieter von Internetzugangsdiensten und öffentlich zugänglichen interpersonellen Kommunikationsdiensten bestimmte Informationen, einschließlich Preise/Tarife und Vertragsdetails, den Verbrauchern nur insoweit bereitzustellen, als ihre Dienste überhaupt Geschäftsbedingungen unterliegen. Diese Bedingung wird in § 50 des Gesetzentwurfs nicht zutreffend widergespiegelt.
- § 50 scheint auch einige Voraussetzungen zu enthalten, die auf Art. 102 Abs. 1 des EECC und den entsprechenden Anhang VIII zurückzuführen sind. Die Anwendung dieser Vorschriften sollte sich jedoch auf Verbraucher beschränken[10]. In dieser Hinsicht sind wir der Ansicht, dass § 50 über die Bestimmung des Art. 102 Abs. 2 EECC hinausgeht. Wir weisen auch darauf hin, dass es eine mögliche Verwechslung mit § 53 Abs. 1 Nr. 1 gibt, der hauptsächlich die gleichen Fragen behandelt und sich richtigerweise eindeutig auf Verbraucherverträge beschränkt.
- § 50 Abs. 2 des Gesetzentwurfs erlaubt auch die Auferlegung „vergleichbarer“ Informationen. In dieser Hinsicht überschneidet sich die Regelung mit der Bestimmung von § 51 des Gesetzentwurfs und Art. 103 Abs. 2 EECC und geht über Art. 103 Abs. 1 EECC hinaus.
- Punkt 2.5 des Anhangs IX EECC weist darauf hin, dass Anbieter von NB-ICS nicht nur Informationen über den Zugang zu Notdiensten/Anruferstandorten bereitstellen sollten, sondern auch „alle Beschränkungen in Bezug auf letzteren“. Dieses Element sollte in § 50 einbezogen werden (siehe auch das nächste Kapitel über Notrufe).
- Soweit § 50 des Gesetzentwurfs die Umsetzung von Art. 104 Abs. 1 EECC zum Ziel hat, muss beachtet werden, dass dieser Artikel es Aufsichtsbehörden gestattet, zusätzliche Veröffentlichungsanforderungen im Hinblick auf QoS (Qualität der Dienste) und Zugänglichkeit an solche Anbieter zu stellen, insoweit sie die Kontrolle über Komponenten des

[10] Abgesehen von Endnutzern werden nach Artikel 102 Abs. 2 diese Informationen eindeutig und ausschließlich nur von Unternehmen verlangt, „... bei denen es sich um Kleinstunternehmen oder kleine Unternehmen oder Organisationen ohne Gewinnerzielungsabsicht handelt, [...], sofern diese nicht ausdrücklich zugestimmt haben, auf die Anwendung diese Bestimmungen ganz oder teilweise zu verzichten”.

Netzes ausüben. DIGITALEUROPE fordert, dass § 50 Abs. 2 des Gesetzentwurfs dahingehend geändert werden sollte, dass der Absatz mit den Regelungen im EECC übereinstimmt, denen der Anbieter in dieser Hinsicht unterliegt.

Wir fordern daher den deutschen Gesetzgeber auf, die Regelungen des § 50 auf die Vorgaben von Artikel 103 Abs. 1 abzustimmen und den Geltungsbereich zu begrenzen, um Verwirrung und mögliche Überschneidungen mit anderen EECC-Regelungen zu vermeiden.

Nach § 65 Abs. 2 des Gesetzentwurfs können Endnutzer Abrechnungen, Einzelverbindungsnachweise oder Abbuchungen eines vorausbezahlten Guthabens innerhalb von 8 Wochen beanstanden. Dies scheint über den EECC hinauszugehen, der keine solche Frist enthält. In Anbetracht der Tatsache, dass dies scheinbar sowohl für Verbraucher- als auch für Geschäftskunden-Verträge gilt, stellt DIGITALEUROPE die Angemessenheit der Aufrechterhaltung dieser Bestimmung in Frage, die aus dem TKG übernommen wurde. Es wäre gerechtfertigt, die Bestimmung zumindest auf Verbraucherverträge zu beschränken, um die Vertragsfreiheit im Geschäftskunden-Bereich zu bewahren.

Notruf (Art. 109 EECC / § 161 Gesetzentwurf)

Der EECC wird insofern korrekt umgesetzt, als die Norm die Anbieter von nummernbasierten interpersonellen Kommunikationsdiensten für ausgehende Anrufe zu Nummern im nationalen oder internationalen Nummerierungsplan verpflichtet, Zugang zu Notrufdiensten zu gewährleisten. Es wird dann der BNetzA überlassen, weitere technische Leitlinien zu entwickeln, wobei hilfreicherweise erwähnt wird, dass diese auf internationalen Standards basieren sollten.

DIGITALEUROPE trägt vor, dass das Gesetz auch auf die Erwägungsgründe (284)-(286) EECC Bezug nehmen sollte, nach denen die Bereitstellung von Notrufdiensten, einschließlich der Übermittlung von Standortinformationen, für bestimmte nummernbasierte Dienste, insbesondere netzunabhängige nummernbasierte Dienste, technisch nicht durchführbar sein könnte: „Solchen netzunabhängigen Anbietern, d. h. Anbietern, die nicht mit einem Anbieter öffentlicher elektronischer Kommunikationsnetze integriert sind, ist es unter Umständen technisch nicht möglich, Angaben zum Anruferstandort bereitzustellen."

Insbesondere die Anwendung der Notrufverpflichtung auf ausgehende One-way-VoIP-Dienste führt zu praktischen Problemen, die sich aus dem in Deutschland etablierten Leitstellen-Routing-Modell ergeben, das auf Routing-Tabellen der BNetzA basiert, die validierte Standortbestimmungsdaten auf Seiten der Teilnehmer erfordern. Während das Vorhandensein solcher zuverlässiger

Standortbestimmungsdaten technisch im Bereich der Festnetztelefonie und in der traditionellen GSM-basierten Mobilkommunikation gewährleistet ist, ist die Situation im Bereich der nummerngebundenen OTT-Dienste grundlegend anders, da diese Apps und Dienste keine festen Standortinformationen haben, die in die Routing-Tabellen eingetragen werden können (da die Dienste nomadisch ausgestaltet sind). Während OTT-Apps Zugriff auf bestimmte Benutzerstandortinformationen haben können – abhängig von den Datenschutzeinstellungen des Benutzers und den Fähigkeiten (z. B. GPS oder andere Geolokalisierungstechnologie) des Geräts, auf dem die App verwendet wird – ist das Notrufsystem in Deutschland nicht so eingerichtet, dass es Notrufe auf der Grundlage dynamisch abgeleiteter Echtzeitstandortinformationen routet. Das System ist so konzipiert, dass das Routing ausschließlich an einem in den Routing-Tabellen vorab ausgefüllten Standort (entweder die Nutzeradresse oder die Adresse der Funkzelle) erfolgt.

Dies wirft die Frage auf, wie der Anbieter eines solchen Dienstes seine Verpflichtung nach § 161 des Gesetzentwurfs erfüllen sollte, wenn die Standortinformationen fehlen, was eine Voraussetzung für die korrekte Weiterleitung an das Kontrollzentrum wäre. Bisher liefert der Gesetzentwurf keine ausreichende Antwort darauf.

Das EECC führt in EG (286) dazu an: „Wenn solche Normen und die zugehörigen Notrufabfragestellen noch nicht eingeführt wurden, sollten für den Zugang zu Notdiensten keine netzunabhängigen nummerngebundenen interpersonellen Kommunikationsdienste erforderlich sein, es sei denn, dies geschieht auf eine Art und Weise, die technisch machbar und wirtschaftlich ist. Dies kann zum Beispiel bedeuten, dass ein Mitgliedstaat eine einzelne zentrale Notrufabfragestelle für den Empfang von Notrufen benennt“.

DIGITALEUROPE schlägt vor, den § 161 Abs. 4 des Gesetzentwurfs klarstellend zu ergänzen, sodass sein Wortlaut mit dem Erwägungsgrund (286) EECC in Einklang gebracht wird. Wir weisen auch darauf hin, dass der Erwägungsgrund (285) EECC deutlich macht, dass es den Mitgliedstaaten freisteht, eine weitere Verfeinerung des Geltungsbereichs der NB-ICS zu implementieren, die Zugang zu Notrufdiensten bieten müssen, wobei die Fähigkeiten und die technische Ausrüstung ihrer Notrufabfragestellen berücksichtigt werden. Die Niederlande haben beispielsweise in ihrem Gesetz derzeit vorgeschlagen, nur von Sprachkommunikationsdiensten die Bereitstellung des Zugangs zu Notrufdiensten zu verlangen.

Die Frage der technischen Machbarkeit wird auch in Anhang IX, 2.5 und Anhang VIII, B II. 1) des EECC erwähnt und angemessen behandelt. Dieser sieht ausdrücklich vor, dass Anbieter von öffentlich zugänglichen nummernbasierten Diensten, die es Endnutzern ermöglichen, Anrufe an eine Nummer in einem nationalen oder internationalen Nummernplan zu tätigen, Informationen

bereitstellen müssen über eventuelle Beschränkungen oder Einschränkungen des Zugriffs auf Notrufdienste oder Standortinformationen, soweit dies auf mangelnder technischer Machbarkeit beruht. Wie bereits im vorherigen Kapitel erwähnt, haben wir darauf hingewiesen, dass § 50 des Gesetzentwurfs diese Präzisierung noch nicht enthält, und wir bitten den Gesetzgeber höflich, dieses Element aufzunehmen, um das Gesetz vollständig mit dem EECC in Einklang zu bringen.

In Bezug auf nummernunabhängige Kommunikationsdienste begrüßen wir, dass der deutsche Umsetzungsentwurf den Geltungsbereich des EECC berücksichtigt und in § 161 des Gesetzentwurfs keine obligatorische Anforderung für solche Dienste einführt, den Zugang zu Notrufdiensten zu bieten.

Daten für Auskunftsersuchen / automatisierte Auskunftsverfahren (§§ 169 und 170 Gesetzentwurf)

Die Umsetzung des EECC bietet dem deutschen Gesetzgeber die Möglichkeit, das Gesetz, das bereits 2012 vom Bundesverfassungsgericht kritisiert wurde[11] zu aktualisieren und zu modernisieren. Diese Kritik ist umso bedeutender angesichts der jüngsten europäischen Rechtsprechung[12], die klar festlegt, dass Anbieter nicht einer voraussetzungslosen Übermittlung oder Speicherung von Verkehrsdaten und Standortdaten unterworfen werden dürfen, auch nicht zum Zweck der Kriminalitätsbekämpfung im Allgemeinen oder zum Schutz der nationalen Sicherheit.

DIGITALEUROPE ist verwundert, dass der Geltungsbereich von § 169 aufgrund des breiteren Geltungsbereichs der EECC-Definition von ECS ausgeweitet wird, anstatt sich dieser Rechtsprechung anzupassen. Genauer gesagt,

---

[11] Im Jahr 2012 prüfte das Verfassungsgericht § 112 TKG (BVerfG 1 BvR 1299/05 – Entscheidung vom 24. Januar 2012) und stellte fest, dass dieser, obwohl er im Allgemeinen rechtsgültig war, „erheblich größeres Eingriffsgewicht erhalten, wenn statische IP-Adressen künftig – etwa auf der Basis des Internetprotokolls Version 6 – in größerem Umfang die Grundlage der Internetkommunikation bilden sollten. (…) Wenn aber in der Praxis auch Privatpersonen in weitem Umfang statische IP-Adressen zugeteilt werden, kann das möglicherweise dazu führen, dass hierdurch generell oder zumindest in weitem Umfang die Identität von Internetnutzern ermittelt und Kommunikationsvorgänge im Netz nicht nur für eine begrenzte Zeit, sondern auch dauerhaft deanonymisiert werden können. Eine solche weitreichende Möglichkeit zur Deanonymisierung der Kommunikation im Internet geht über die Wirkung eines traditionellen Rufnummernregisters hinaus“.

Das Gericht warnte ausdrücklich vor der zentralen Speicherung von Kennungen wie statischen IP-Adressen: „Angesichts dieses erhöhten Informationspotenzials wäre die generelle Möglichkeit der Identifizierung von IP-Adressen nur unter engeren Grenzen verfassungsrechtlich zulässig (vgl. BVerfGE 125, 260 <343 f., 356 ff.>). Den Gesetzgeber trifft insoweit eine Beobachtungs- und gegebenenfalls Nachbesserungspflicht“.

[12] Rechtssache C-623/17 und verbundene Rechtssachen C-511/18, C-512/18 und C-520/18.

- verpflichtet § 169 Abs. 1 des Gesetzentwurfs – wie sein Vorgänger § 111 TKG – Dienste, die ihren Kunden Nummern zuweisen, die personenbezogenen Daten ihrer Kunden zu erfassen und zu speichern, wie etwa Name und Adresse sowie Geburtsdatum des Teilnehmers, zusammen mit seiner Telefonnummer, anderen Zugangskennungen (*Anschlusskennungen*), die der Anbieter zugewiesen hat, Identifikationsnummern von mobilen Geräten, wenn diese vom gleichen Dienstanbieter bereitgestellt werden, und Vertragsdatum. Identität und Adresse müssen durch Personalausweise, Aufenthaltsgenehmigungen usw. verifiziert werden. Alle Kosten für die Erhebung und Speicherung sind vom Anbieter zu tragen.
- Gemäß § 170 Abs. 1 sollen die Daten – wie beim Vorgänger § 112 TKG – in einer zentralen Datenbank gespeichert werden, auf die die BNetzA Zugriff hat. In ihrem letzten Tätigkeitsbericht erklärt die BNetzA: „Im Jahr 2018 wurden 13,94 Millionen Ersuchen über das AAV bei der Bundesnetzagentur beauskunftet. Im Vergleich zum Vorjahr wurden damit rund 1,2 Millionen Ersuchen mehr an die Bundesnetzagentur gestellt und von dieser beantwortet. Für das Jahr 2019 wird wieder eine Steigerung erwartet. “[13] Diese Verpflichtung erscheint besonders intrusiv im Hinblick auf die Privatsphäre, was insbesondere hinsichtlich der oben erwähnte Rechtsprechung fragwürdig erscheint.

Um unverhältnismäßige Verpflichtungen zu vermeiden, schlägt DIGITALEUROPE vor, OTT-Anbieter, insbesondere nummerunabhängige, aber auch netzunabhängige nummernbasierte Dienste, von den in den oben genannten Bestimmungen enthaltenen Datenspeicherungsverpflichtungen und direkten behördlichen Zugriffmöglichkeiten auszunehmen – mindestens bis zu einem Zeitpunkt, zu dem es mehr Klarheit über den Umfang der Datenspeicherungsverpflichtungen und -regelungen in der EU gibt.

Sollte der Gesetzgeber - trotz der vorstehend dargelegten verfassungsrechtlichen und sonstigen Bedenken - beabsichtigen, die starren Verpflichtungen über den direkten behördlichen Zugriff und die sonstigen Verpflichtungen von Teil 10 des Gesetzentwurfs auf nummernunabhängige Dienste auszudehnen, ist DIGITALEUROPE der Ansicht, dass eine Übergangsfrist von mindestens 12 Monaten erforderlich ist, damit die betroffenen Diensteanbieter sich auf die Umsetzung vorbereiten können.

DIGITALEUROPE stellt fest, dass das 2012 vom Bundesverfassungsgericht erwartete Risiko sich verwirklicht hat. Aufgrund der Einführung von IPv6 können

[13] Tätigkeitsbericht der BNetzA 2018/2019, Seite 237, verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Taetigkeitsberichte/2019/TK_20182019.pdf?__blob=publicationFile&v=9

Nutzern zunehmend statische IP-Adressen zugewiesen werden. Das „traditionelle Rufnummernregister“, das die deutsche Gesetzgebung 1996 (in § 90 des TKG 1996) vorgesehen hatte, wurde durch die Entwicklung des Internets in eine Datenbank umgewandelt, die zur Überwachung der Kommunikationsgewohnheiten der deutschen Bürger verwendet werden kann. Aus diesem speziellen Grund hatte das Bundesverfassungsgericht davor gewarnt, weiterhin andere Kennungen als Telefonnummern in die Datenbank aufzunehmen.

Der Gesetzentwurf berücksichtigt auch in keiner Weise den besonderen Charakter der automatisierten Datenherausgabe. Anfragen werden über elektronische Schnittstellen gestellt, ohne dass der Anbieter ein förmliches Ersuchen erhält und ohne dass er erfährt, welche Daten welches Nutzers betroffen sind. Die BNetzA ruft die Daten direkt ab und leitet sie an die anfragenden Behörden weiter.

§ 170 des Gesetzentwurfs ist eine Konstellation des „direkten Zugangs“, bei der die Behörden direkten technischen Zugang zu den Kundendaten der Anbieter haben, die in der Praxis keine Möglichkeit haben, eine einzelne Anfrage zu prüfen, um zu entscheiden, ob sie Rechtsschutz in Anspruch nehmen wollen. Im Widerspruch zu diesem rechtlich außergewöhnlichen Charakter hat sich der Vorgänger von § 170 bereits zu einem Massenabfrageinstrument ohne jegliche Transparenz für die Nutzer, die Anbieter oder die allgemeine Öffentlichkeit entwickelt. Das einzige bekannte Transparenzinstrument ist ein kurzer Hinweis im jährlichen Tätigkeitsbericht der BNetzA über die Gesamtzahlen, ohne Informationen über die Art der zugrunde liegenden Anfragen.

Der Gesetzentwurf würde jedoch den Geltungsbereich dieser Bestimmung weiter ausdehnen. Gemäß § 169 (3) müssen Anbieter von nummernunabhängigen Diensten, wenn sie solche personenbezogenen Daten erheben, ihre Nutzer in diese Datenbank aufnehmen. Da diese Anbieter keine Telefonnummern verwenden, wären sie verpflichtet, eine andere Nutzeridentifikation („*Kennung*“) zu speichern. In vielen Fällen verwenden nummernunabhängige Dienste Online-Benutzernamen, *nicknames* oder Kontonamen als eindeutige Kennungen. Oft entscheiden sich Nutzer dafür, denselben Benutzernamen über verschiedene Plattformen und Dienste hinweg zu verwenden, auch für Inhalts- und andere Nicht-Kommunikationsdienste, was die Auswirkungen auf ihre verfassungsmäßig garantierten Rechte verstärkt, falls solche Kennungen zentral erfasst und gespeichert werden. Aus diesen Gründen fordert DIGITALEUROPE den deutschen Gesetzgeber höflich auf, die Einbeziehung von Kennungen in § 169 (3) des Gesetzentwurfs nochmals zu überdenken.

Darüber hinaus geht DIGITALEUROPE davon aus, dass der aktuelle Wortlaut von § 169 (3) sich auf Nutzerdaten bezieht, die Anbieter von nummernunabhängigen Diensten im Verlauf der Bereitstellung dieser NI-ICS

erfasst. *(„für denjenigen, der nummernunabhängige interpersonelle Telekommunikationsdienste erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1 und 3 erhebt“)*. Anbieter von nummernunabhängigen Diensten können aber auch Inhalts- und andere Nicht-Kommunikationsdienste, einschließlich E-Commerce-Dienste, anbieten, bei denen sie oft zu Abrechnungszwecken Daten erfassen, einschließlich Namen und Adressen. Diese Daten werden indes nicht im Rahmen der Bereitstellung des Kommunikationsdienstes erhoben und sollten daher nicht nach § 169 (3) des Gesetzentwurfs gespeichert werden. Diese wichtige Einschränkung ist jedoch möglicherweise nach dem aktuellen Wortlaut („*dabei*“) nicht hinreichend klar. Sollte § 169 (3) im Wesentlichen in seiner aktuellen Form bleiben, schlägt DIGITALEUROPE daher eine ausdrückliche Erklärung in der Begründung vor, dass die Verpflichtung nur für diejenigen Daten gilt, die ausschließlich im Rahmen der Bereitstellung des betreffenden nummernunabhängigen Dienstes erfasst werden.

DIGITALEUROPE vertritt außerdem die Auffassung, dass zwischen Verbraucherdiensten und Geschäftskunden-Diensten unterschieden werden muss. Im letzteren Fall sind der Kunde und der Endnutzer nicht in jedem Fall identisch. Dies schränkt die Daten ein, die dem Anbieter über Endnutzer vorliegen.

Manuelles Auskunftsverfahren (§ 171 Gesetzentwurf)

DIGITALEUROPE legt Wert auf die Notwendigkeit der Zusammenarbeit zwischen Strafverfolgungsbehörden und Anbietern von ECS. Ein manuelles Verfahren zur Herausgabe von Nutzerdaten, das es Anbietern ermöglicht, rechtmäßigen Zugriff auf die Daten zu gewährleisten, die die Nutzer ihnen anvertraut haben, ist besser geeignet, deren Rechte zu schützen, als ein automatisiertes Verfahren, wie das in §§ 169 und 170 des Gesetzentwurfs beschriebene. Allerdings würde § 171 des Gesetzentwurfs von einigen Klarstellungen profitieren, zusätzlich zu den Änderungen, die für die Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 erforderlich werden. Im Einzelnen:

- Die in § 171 vorgesehene manuelle Datenherausgabe umfasst Daten wie Passwörter, PINs und Bildschirmentsperrcodes. DIGITALEUROPE bittet darum, in der Begründung ausdrücklich darauf hinzuweisen, dass diese Daten einen besonderen Schutz genießen, der sie unkenntlich und auch für die Anbieter von ECS nicht reproduzierbar machen sollte.
- Die aktuelle Fassung von § 171 Abs. 5 des Gesetzentwurfs verlangt, dass die Anbieter sicherstellen, dass jede Behördenanfrage durch eine

verantwortliche Fachkraft auf Einhaltung der formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird. Nach Ansicht von DIGITALEUROPE sollten sich die Anbieter indes auf ein rechtmäßges Verwaltungshandeln verlassen können. Aus der Praxis sind zahlreiche Anfragen auf Grundlage von § 113 TKG bekannt, die sich auf Daten beziehen, die eindeutig nicht durch § 113 TKG abgedeckt sind, wie z. B. Protokolldateien, IP-Adressen, Datum und Uhrzeit der letzten Anmeldung, bekannte E-Mail-Adressen der betroffenen Person bei anderen Anbietern und Identität der Behörden, die bereits nach denselben Daten gefragt haben. Dementsprechend müssen sich die Provider bereits heute mit zahlreichen Anfragen befassen, die nicht im Einklang mit § 113 TKG stehen. Um sicherzustellen, dass die Verantwortung im Zusammenhang mit der manuellen Datenherausgabe angemessen verteilt wird, bittet DIGITALEUROPE höflich, dass § 171 (2) (Satz 4) – der derzeit lautet: „Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen“ – entsprechend geändert wird, um widerzuspiegeln, dass die Behörden nicht nur für die *Zulässigkeit* der Anträge verantwortlich sind, sondern auch dafür, dass der Antrag im Wesentlichen inhaltlich gerechtfertigt ist (*Begründetheit*).

FÜR WEITERE INFORMATIONEN WENDEN SIE SICH BITTE AN:

Alberto Di Felice

Direktor für Infrastruktur, Datenschutz und Sicherheit

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Über DIGITALEUROPE

DIGITALEUROPE repräsentiert die digitale Technologiebranche in Europa. Zu unseren Mitgliedern gehören einige der weltweit größten IT-, Telekommunikations- und Unterhaltungselektronikunternehmen sowie nationale Verbände aus allen Teilen Europas. DIGITALEUROPE möchte, dass europäische Unternehmen und Bürger in vollem Umfang von digitalen Technologien profitieren und dass Europa die besten digitalen Technologieunternehmen der Welt aufbauen, anziehen und erhalten kann. DIGITALEUROPE stellt die Beteiligung der Industrie an der Entwicklung und Umsetzung der EU-Richtlinien sicher.

DIGITALEUROPE Mitgliedschaft

Mitgliedsunternehmen

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

Nationale Wirtschaftsverbände

Belgien: AGORIA
Dänemark: DI-Digital, IT BRANCHEN, Dansk Erhverv
Deutschland: BITKOM, ZVEI
Estland: ITL
Finnland: TIF
Frankreich: AFNUM, Syntec Numérique, TECH IN France
Griechenland: SEPE
Irland: Technology Ireland
Italien: Anitec-Assinform
Kroatien: Kroatische Wirtschaftskammer
Litauen: INFOBALT
Luxemburg: APSI
Niederlande: NLdigital, FIAR
Norwegen: Abelia
Österreich: IOÖ
Polen: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Rumänien: ANIS, APDETIC
Schweden: Teknikföretagen, IT&Telekomföretagen
Schweiz: SWIKO
Slowakei: ITAS
Slowenien: GZS
Spanien: AMETIC
Türkei: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
Ungarn: IVSZ
Vereinigtes Königreich: techUK
Weißrussland: INFOPARK
Zypern: CITEA