Rat der
Europäischen Union

Brüssel, den 2. November 2021
(OR. en)

13413/21

MI 794
ENT 178
ECO 117
IND 312
TELECOM 399
DELACT 236

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	29. Oktober 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	C(2021) 7672 final
Betr.:	DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION vom 29.10.2021 zur Ergänzung der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, auf die in Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie Bezug genommen wird

Die Delegationen erhalten in der Anlage das Dokument C(2021) 7672 final.

Anl.: C(2021) 7672 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 29.10.2021
C(2021) 7672 final

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 29.10.2021

zur Ergänzung der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, auf die in Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie Bezug genommen wird

(Text von Bedeutung für den EWR)

{SEC(2021) 382 final} - {SWD(2021) 302 final} - {SWD(2021) 303 final}

BEGRÜNDUNG

1. KONTEXT DES DELEGIERTEN RECHTSAKTS

Täglich wird eine große Zahl an Funkanlagen genutzt, und zwar nicht nur von erwachsenen Verbrauchern oder gewerblichen Nutzern, sondern auch von schutzbedürftigen Nutzern wie Kindern.

Einerseits haben das Europäische Parlament und der Rat wiederholt darauf hingewiesen, dass die Cybersicherheit in der EU gestärkt werden muss[1] und dabei die zunehmende Bedeutung von vernetzten Funkanlagen, einschließlich Maschinen, Sensoren und Netzwerken, die das Internet der Dinge (Internet of Things, IoT) bilden, sowie die damit verbundenen Sicherheitsprobleme anerkannt. Der EU-Rahmen umfasst mehrere Rechtsakte,[2] die Aspekte der Cybersicherheit oder einige ihrer Elemente abdecken. Bei der Behandlung bestimmter Fragen der Cybersicherheit können für verschiedene Akteure bzw. Interessenträger bestimmte Verpflichtungen gelten, mit denen ein Beitrag zur Gewährleistung der Sicherheit des gesamten Ökosystems geleistet werden soll. Netzbetreiber und Diensteanbieter sollten beispielsweise sicherstellen, dass ihre Systeme und Plattformen sicher sind, die Hersteller von Anlagen sollten sicherstellen, dass diese unter Berücksichtigung der Sicherheitsgrundsätze konzipiert werden, die Nutzer sollten sich der Risiken bei der Ausführung bestimmter Vorgänge und der Notwendigkeit der erforderlichen Aktualisierungen der von ihnen verwendeten Anlagen bewusst sein, und die Mitgliedstaaten können Prioritäten setzen. Die Cybersicherheit des gesamten Ökosystems wird nur gewährleistet, wenn alle Komponenten Cybersicherheit bieten.

Andererseits bewertete der norwegische Verbraucherrat im Dezember 2016 die technischen Merkmale ausgewählter, per Funk verbundener Spielzeuge.[3] Die Ergebnisse deuten auf einen möglicherweise mangelhaften Schutz der Rechte der Kinder in Bezug auf die Privatsphäre, den Schutz personenbezogener Daten und die Sicherheit hin. Dank integrierter Lautsprecher, Mikrofone und anderer Sensoren handelt es sich bei vernetzten Spielzeugen per definitionem um „intelligente“ Spielzeuge, die beispielsweise in der Lage sind, Sprache zu interpretieren,

---

[1] Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G, https://op.europa.eu/de/publication-detail/-/publication/02f351c6-1b47-11ea-8c1f-01aa75ed71a1/language-de.
Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G, https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/connected-digital-single-market/file/cyber-security-package.
https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/
http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf.

[2] Dies sind insbesondere: i) die Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO), ii) die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), iii) die Verordnung (EU) 2019/881 („Rechtsakt zur Cybersicherheit“), iv) die Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, v) die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme, vi) die Richtlinie (EU) 2016/1148 über das Sicherheitsniveau von Netz- und Informationssystemen („NIS-Richtlinie“) und vii) die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt („eIDAS-Verordnung“).

[3] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

um mit dem Kind interagieren zu können. Darüber hinaus könnten sie nicht nur Fotos, Videos, Geolokalisierungsdaten und Daten über die Spielerfahrung aufzeichnen, sondern auch Daten zur Herzfrequenz, den Schlafgewohnheiten oder andere biometrische Daten. Aus dem Bericht geht ferner hervor, dass einige dieser Spielzeuge bei der Interaktion mit dem Kind auch für Produkte werben können, was möglicherweise nicht mit der von dieser Art von Produkten zu erwartenden Transparenz im Einklang steht. Aus diesem Grund haben die europäischen Verbraucherverbände[4] zum Handeln aufgerufen.

Spielzeuge sind nur ein Teil eines größeren Sektors, der ähnliche Risiken birgt. In der Richtlinie 2009/48/EG sind die Sicherheitsanforderungen festgelegt, die von dem Spielzeug, das in den Anwendungsbereich der genannten Richtlinie fällt, erfüllt werden müssen, bevor es in der Union vermarktet werden darf. Die Anforderungen dieser Richtlinie enthalten jedoch beispielsweise keine Bestimmungen, die den Schutz personenbezogener Daten und der Privatsphäre oder den Schutz vor Betrug gewährleisten.

Smarte Geräte, smarte Kameras und eine Reihe anderer vernetzter Funkanlagen wie Mobiltelefone, Laptops, Dongles, Alarmanlagen und Hausautomatisierungssysteme sind ebenfalls Beispiele für Geräte, bei denen die Gefahr besteht, dass sie gehackt werden und dass Datenschutzprobleme entstehen, wenn sie mit dem Internet verbunden sind. Darüber hinaus können tragbare Funkanlagen (z. B. Ringe, Armbänder, Taschenclips, Headsets, Fitnesstracker usw.) eine Reihe sensibler Daten des Nutzers über einen längeren Zeitraum überwachen und registrieren (z. B. Standort, Temperatur, Blutdruck, Herzfrequenz) und diese nicht nur über das Internet, sondern auch über unsichere Nahbereichs-Kommunikationstechnologien weiter übertragen. Die Funkanlagenrichtlinie 2014/53/EU[5] schafft einen Rechtsrahmen für das Inverkehrbringen von Funkanlagen im Binnenmarkt. Es werden verbindliche Marktzugangsbedingungen für Funkanlagen festgelegt. Die Funkanlagenrichtlinie gilt für Elektro- und Elektronikgeräte, die Funkfrequenzen für Kommunikations- und/oder Funkortungszwecke nutzen können. Die Mitgliedstaaten ergreifen über ihre nationalen Marktüberwachungsbehörden Korrekturmaßnahmen in Bezug auf nichtkonforme Funkanlagen.

In Artikel 3 der Funkanlagenrichtlinie sind die grundlegenden Anforderungen festgelegt, die Funkanlagen, die in der Union in Verkehr gebracht werden, erfüllen müssen, wobei Artikel 3 Absatz 1 Buchstabe a grundlegende Anforderungen in Bezug auf Gesundheit und Sicherheit, Artikel 3 Absatz 1 Buchstabe b grundlegende Anforderungen an die elektromagnetische Verträglichkeit und Artikel 3 Absatz 2 grundlegende Anforderungen in Bezug auf die effektive und effiziente Nutzung von Funkfrequenzen festlegt. Darüber hinaus sieht Artikel 3 Absatz 3 zusätzliche grundlegende Anforderungen vor, die für die Kategorien oder Klassen von Funkanlagen gelten, die in dem bzw. den entsprechenden delegierten Rechtsakten der Kommission festgelegt sind.

Mit der Funkanlagenrichtlinie wird der Kommission die Befugnis übertragen, delegierte Rechtsakte zu erlassen, um eine der grundlegenden Anforderungen nach Artikel 3 Absatz 3 der Funkanlagenrichtlinie anzuwenden, wobei darin festgelegt wird, welche Kategorien oder

[4] http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

[5] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62).

Klassen von Funkanlagen von den einzelnen Anforderungen betroffen sind. Die folgenden drei Buchstaben von Artikel 3 Absatz 3 zweiter Unterabsatz sind für diese Initiative relevant:

- Artikel 3 Absatz 3 Buchstabe d: Schutz des Netzes,
- Artikel 3 Absatz 3 Buchstabe e: Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre,
- Artikel 3 Absatz 3 Buchstabe f: Schutz vor Betrug.

Das Ziel besteht jedoch nicht darin, zusätzliche oder sich überschneidende Vorschriften zu bestehenden Rechtsvorschriften zu schaffen, sondern sicherzustellen, dass die bestehenden Grundsätze gegebenenfalls in spezifische Anforderungen für die Herstellung von Produkten umgesetzt werden, die auf dem Unionsmarkt in Verkehr gebracht werden sollen, und zwar mit einem gewissen Grad an Durchsetzbarkeit oder Überprüfbarkeit. Wichtig ist, die Komplementarität mit dem bestehenden EU-Rahmen sicherzustellen. In dieser Hinsicht sollten Funkanlagen, Produkte oder Komponenten, auf die die Verordnungen (EU) 2019/2144[6] und (EU) 2018/1139[7] oder die Richtlinie (EU) 2019/520[8] Anwendung finden, nicht zu den Kategorien oder Klassen von Funkanlagen gehören, die die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben e und f der Richtlinie 2014/53/EU erfüllen sollten.

Was den Datenschutz betrifft, so regeln die Rechtsvorschriften der Union über personenbezogene Daten und den Schutz der Privatsphäre, wie die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[9] und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[10], die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre, aber nicht das Inverkehrbringen von Funkanlagen in der Union.

---

6 Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission (ABl. L 325 vom 16.12.2019, S. 1).

7 Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1).

8 Richtlinie (EU) 2019/520 des Europäischen Parlaments und des Rates vom 19. März 2019 über die Interoperabilität elektronischer Mautsysteme und die Erleichterung des grenzüberschreitenden Informationsaustauschs über die Nichtzahlung von Straßenbenutzungsgebühren in der Union (ABl. L 91 vom 29.3.2019, S. 45).

9 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

10 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Hauptziel dieser Initiative ist es, zur Stärkung des „Ökosystems des Vertrauens“ beizutragen, das sich aus den Synergien aller damit zusammenhängenden EU-Rechtsvorschriften zum Schutz des Netzes, der Privatsphäre und vor Betrug ergibt, die in der begleitenden Folgenabschätzung näher erläutert werden. Durch diese Initiative sollten dann auf dem EU-Markt nur solche Funkanlagen zugelassen werden, die ausreichend sicher sind. Im Hinblick auf die allgemeinen Ziele sollen mit der Initiative die Achtung bestimmter Grundrechte (z. B. des Schutzes der Privatsphäre) gestärkt und die politischen Ziele unterstützt werden, die in anderen EU-Rechtsvorschriften, in denen keine Möglichkeit zur Durchsetzung auf dem Markt vorgesehen ist, festgelegt sind. Angesichts des Ausmaßes der Risiken und der positiven Wirkung, die eine rasche Anwendbarkeit auf die bestehenden politischen Ziele der EU hat, ist auch ein rechtzeitiges Handeln erforderlich. Dadurch, dass bestehende Befugnisse, die der Kommission bereits übertragen wurden, genutzt werden können, ist unter Berücksichtigung des gegebenen Rahmens ein Handeln möglich, ohne dass spezifische zusätzliche Rechtsvorschriften erforderlich sind. Damit die Probleme bei Produkten, die über keine Sicherheitsmerkmale verfügen, angegangen werden können, besteht ein spezifisches Ziel darin, den Marktüberwachungsbehörden ein Durchsetzungsinstrument an die Hand zu geben, mit dem sie Korrekturmaßnahmen ergreifen können. Ein weiteres Ziel besteht darin, einen Binnenmarkt für die betreffenden Produkte zu gewährleisten, der nicht durch unterschiedliche lokale oder nationale Vorschriften behindert wird, die den Verwaltungsaufwand vor allem für kleinere Unternehmen erhöhen. Ein letztes Ziel ist die Schaffung gleicher Wettbewerbsbedingungen durch klare und angemessene Vorschriften, die in der gesamten EU wirksam und einheitlich durchgesetzt werden.

In der Gemeinsamen Mitteilung der Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik vom 16. Dezember 2020 über die Cybersicherheitsstrategie der EU für die digitale Dekade wird die Notwendigkeit von Binnenmarktvorschriften hervorgehoben, die Schutzvorkehrungen gegen unsichere Produkte und Dienste enthalten.[11]

2. KONSULTATIONEN VOR ANNAHME DES RECHTSAKTS

Bei der Konsultationsstrategie für diese Initiative wurden alle möglichen damit zusammenhängenden Aspekte berücksichtigt – auch im Hinblick auf die Auswirkungen auf die Gesellschaft (z. B. Verbraucher und Wirtschaftsakteure) – sowie die nationalen Behörden, die Bedingungen für den Zugang zum Binnenmarkt und die Umsetzung von oder Synergien mit zusätzlichen EU-Rechtsvorschriften. Die Rückmeldungen der Interessenträger wurden zusätzlich zu den Erkenntnissen aus anderen Forschungsquellen (z. B. Fachliteraturrecherche) herangezogen.

Die relevanten Interessenträger waren: Behörden, die für Datenverarbeitung, Betrug und/oder Funkanlagen zuständig sind, Verbände von Wirtschaftsakteuren, einzelne Wirtschaftsakteure, Verbraucherorganisationen, Bürgerinnen und Bürger, akademische Einrichtungen/Forschungseinrichtungen und einschlägige Nichtregierungsorganisationen, benannte Stellen und europäische Normungsorganisationen.

[11] JOIN(2020) 18 final.

Folgende spezifische Konsultationstätigkeiten wurden durchgeführt:

- Alle interessierten Interessenträger konnten über einen Zeitraum von vier Wochen Rückmeldungen zur ersten Folgenabschätzung geben.[12]
- Auf dem Portal „Bessere Rechtsetzung“ der Kommission wurde eine öffentliche Konsultation durchgeführt, die sich über zwölf Wochen erstreckte.[13]
- Eine gezielte Konsultation richtete sich speziell an Mitgliedstaaten, Wirtschaftsakteure (Verbände oder einzelne Wirtschaftsakteure), Verbraucherorganisationen, Konformitätsbewertungsstellen, Verbraucher und andere Experten.

Es wurden auch Interessenträger zur Teilnahme an der gezielten Umfrage eingeladen, darunter jene, die an der Sitzung der Sachverständigengruppe für Funkanlagen teilgenommen haben. 56 von ihnen haben den Fragebogen ausgefüllt. Die 56 Auskunftgebenden kamen aus 20 Ländern, darunter 14 EU-Mitgliedstaaten. Die meisten Antworten (14) kamen aus Belgien, und zwar fast ausschließlich von Verbänden, die Hersteller oder Verbraucher vertreten. Deutschland rangierte mit elf Auskunftgebenden, von denen die meisten Hersteller waren, an zweiter Stelle. Unter den Nicht-EU-Mitgliedstaaten waren die USA mit fünf Auskunftgebenden am stärksten vertreten, darunter waren sowohl Hersteller als auch Industrieverbände. Es gab ein ausgewogenes Verhältnis hinsichtlich der Größe der beteiligten Organisationen. Bei den großen Organisationen handelte es sich ausschließlich um Hersteller oder nationale öffentliche Verwaltungen, mit Ausnahme von zwei Konformitätsbewertungsstellen und einer Universität. Bei vielen der Mikroorganisationen handelte es sich um Branchen- oder Verbraucherverbände. Die Gruppe der kleinen und mittleren Organisationen enthielt eine Mischung aus allen Arten von Organisationen.

An der laufenden öffentlichen Konsultation, die aus offenen und geschlossenen Fragen bestand, beteiligten sich insgesamt 42 Personen. Dabei ergab sich folgendes Länderprofil der Auskunftgebenden:

- Die 42 Auskunftgebenden kamen aus 14 EU-Mitgliedstaaten.
- Die meisten Antworten (acht) kamen aus Deutschland, sieben davon stammten von Bürgerinnen und Bürgern.
- Sechs Antworten kamen aus Belgien und stammten alle von Vertretungsorganen auf EU-Ebene (fünf Wirtschaftsverbände und ein Verbraucherverband).
- Sechs Antworten stammten aus Spanien, vier davon von Behörden und zwei von Unternehmen.
- Keiner der Auskunftgebenden war außerhalb der EU ansässig.

Die Auskunftgebenden entsprachen folgenden Profilen:

[12] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Smartwatches-and-connected-toys

[13] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Smartwatches-and-connected-toys/public-consultation

- Von den 42 Auskunftgebenden waren etwas mehr als die Hälfte (22) Bürgerinnen und Bürger.
- Die Bürgerinnen und Bürger kamen aus zehn EU-Mitgliedstaaten.
- Von den sechs Behörden stammten vier aus Spanien und jeweils eine aus Estland und Irland.
- Von den sieben Wirtschaftsverbänden waren fünf Organe auf EU-Ebene mit Sitz in Belgien.
- Die sechs Unternehmen kamen aus fünf verschiedenen Ländern. Sie bestanden aus drei Kleinstunternehmen, zwei kleinen und einem großen Unternehmen.
- Es gab eine Verbraucherorganisation, bei der es sich um ein Organ auf EU-Ebene mit Sitz in Belgien handelte.

Die Konsultation der Sachverständigengruppe für Funkanlagen (E03587) fand am 18. September 2020 und am 17. November 2020 statt; die Sachverständigengruppe wurde zu vorläufigen Dokumenten konsultiert, die sich mit den wichtigsten Punkten des Delegierten Rechtsakts (Anwendungsbereich, anwendbare Artikel, Ausnahmen, Datum der Anwendbarkeit) befassen. Die Sachverständigengruppe wurde am 24. Februar 2021 zu dem Entwurf des Rechtsakts konsultiert. An der Sachverständigengruppe für Funkanlagen nehmen Behörden der EU-Mitgliedstaaten und assoziierter Länder, Verbraucherverbände, Verbände der Wirtschaftsakteure, die sich mit der Funkanlagenrichtlinie befassen, sowie europäische Normungsorganisationen teil. Die eingegangenen Stellungnahmen sind auf CIRCABC öffentlich zugänglich,[14] wo auch die entsprechenden Diskussionen in den Sitzungsprotokollen zusammengefasst sind.

Einige Optionen wurden entweder zu einem frühen Zeitpunkt oder während der Entwicklung dieser Initiative aus verschiedenen Gründen (wie im Folgenden erläutert) verworfen:

- Zu einem frühen Zeitpunkt wurde die Einführung eines horizontalen Rechtsakts zur Cybersicherheit als eine weitere Option erwogen. Mehrere einzelne Hersteller und ihre Branchenverbände haben dies als die beste Option vorgeschlagen, die ihrer Ansicht nach eine Fragmentierung der Ergebnisse, Effizienz und Wirksamkeit verhindern würde. Es wurde jedoch beispielsweise in den Diskussionen der Sachverständigengruppe für Funkanlagen darauf hingewiesen, dass eine solche Option – realistisch gesehen – angesichts der für ein Mitentscheidungsverfahren erforderlichen Fristen für die Gesetzgebung nicht so zeitnah sein könnte wie ein oder mehrere delegierte Rechtsakte im Rahmen der Funkanlagenrichtlinie.
- Zum Zeitpunkt der Veröffentlichung der Folgenabschätzung in der Anfangsphase war der Rechtsakt zur Cybersicherheit noch nicht verabschiedet, sodass keine Optionen auf dieser Rechtsvorschrift basieren konnten. Darüber hinaus schafft die Einführung von Systemen zur Zertifizierung der Cybersicherheit im Rahmen des Rechtsakts keine rechtlichen Verpflichtungen in Bezug auf das Inverkehrbringen von Produkten. Die Zertifizierung der Cybersicherheit bleibt daher ein freiwilliger Akt. Sie wurde im Rahmen der freiwilligen Maßnahmen der Industrie im Zusammenhang mit den Optionen behandelt.

[14] https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/f6e8f574-6864-4350-94bb-1719fe29a6c0?p=1&n=10&sort=modified_DESC

Schließlich schlugen einige Mitgliedstaaten zu einem späteren Zeitpunkt, d. h. nach der Veröffentlichung der Folgenabschätzung in der Anfangsphase, vor, Artikel 3 Absatz 3 Buchstabe d in Verbindung mit Artikel 3 Absatz 3 Buchstabe e und Artikel 3 Absatz 3 Buchstabe f anzunehmen, wobei sie auf den Synergieeffekt hinwiesen, der sich aus einer gemeinsamen Annahme der drei Artikel ergeben würde. Da die Mitgliedstaaten und die Verbraucherverbände die Annahme von Artikel 3 Absatz 3 Buchstabe d als Ergänzung zu Option 4 betrachteten, wurde eine eigenständige Option für Artikel 3 Absatz 3 Buchstabe d nicht in Erwägung gezogen.

Um die Cybersicherheitsrisiken bei allen vernetzten Produkten und verbundenen Diensten sowie auf ihren gesamten Lebenszyklus bezogen anzugehen, hat die Kommission in der Gemeinsamen Mitteilung vom Dezember 2020 über die Cybersicherheitsstrategie der EU für die digitale Dekade[15] angekündigt, dass sie ein umfassendes Herangehen in Erwägung ziehen wird, möglicherweise auch neue horizontale Vorschriften zur Verbesserung der Cybersicherheit aller vernetzten Produkte und zugehörigen Dienste im Binnenmarkt.

3. ÖFFENTLICHE KONSULTATION ZUM ENTWURF DES RECHTSAKTS

Nach Erörterung des Entwurfs mit der Sachverständigengruppe für Funkanlagen wurde eine formelle vierwöchige öffentliche Konsultation[16] eingeleitet. Die Konsultation stand allen Bürgern und Interessenträgern ohne Einschränkungen offen.

Die endgültige Zahl der eingegangenen Beiträge belief sich auf 26. Dabei ergab sich folgendes Länderprofil der Auskunftgebenden:

- Die meisten Antworten (18) kamen aus Belgien.
- Nur ein Beitrag wurde von außerhalb der Europäischen Union (Schweiz) übermittelt.
- Die übrigen Antworten stammten aus den Niederlanden (4), Polen (1), Deutschland (1) und Frankreich (1).

Die Auskunftgebenden entsprachen folgenden Profilen:

- Die meisten Beiträge (17) stammten von der Industrie.
- Verbraucher und nichtstaatliche Vereinigungen reichten 3 Antworten ein.
- 4 Bürger übermittelten Rückmeldungen.
- 2 Beiträge gingen von den europäischen Normungsorganisationen ein.

Nach Prüfung dieser Beiträge wurde der Schluss gezogen, dass es aus den nachstehend dargelegten Gründen nicht erforderlich ist, den Entwurf des Rechtsakts zu ändern:

- Einige Beiträge zielten speziell auf technische Maßnahmen zur Minderung von Cybersicherheitsbedrohungen ab. Dieser Rechtsakt enthält jedoch keine technischen Maßnahmen, sondern lediglich grundlegende Anforderungen. Die in den eingegangenen Beiträgen zu diesen technischen Fragen geäußerten Meinungen werden bei der Ausarbeitung der unterstützenden harmonisierten Normen berücksichtigt.

[15] JOIN(2020) 18 final.

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Internet-connected-radio-equipment-and-wearable-radio-equipment_en

- Einige Interessenträger äußerten Bedenken in Bezug auf die vermeintliche Überschneidung von Verpflichtungen mit anderen EU-Rechtsvorschriften. Mit diesem Entwurf wird das Inverkehrbringen der in den Anwendungsbereich fallenden Anlagen geregelt, während dieses Element durch den übrigen EU-Rechtsrahmen nicht geregelt ist. Darüber hinaus sollen mit dem Rechtsakt weder Verfahren oder Dienste noch Fragen hinsichtlich des Inverkehrbringens geregelt werden, die nicht unter die Funkanlagenrichtlinie fallen.
- Ein Industrieverband wies darauf hin, dass der Rechtsakt seiner Ansicht nach Hindernisse für KMU schaffe. Wie in der Folgenabschätzung angegeben, werden die künftigen harmonisierten Normen die technischen Lösungen liefern. KMU werden zu ihrer Entwicklung beitragen.
- Es gingen mehrere Stellungnahmen zum Verständnis der Kategorien von Anlagen ein, für die die grundlegenden Anforderungen gelten werden. Die Definition des Begriffs „mit dem Internet verbundenes Gerät“ wurde in der zuständigen Sachverständigengruppe ausführlich erörtert. Die Einschränkung des Anwendungsbereichs in Bezug auf die beabsichtigte Verwendung und nicht auf die technischen Fähigkeiten bedeutet, dass mehrere Anlagen nicht unter den Rechtsakt fallen würden. Aus technischer Sicht wäre eine Kommunikation über das Internet möglich, und Hacker könnten diese Schwachstellen ausnutzen. Darüber hinaus ist der Begriff „Netz“ klar und umfasst das Internet.
- Einige Industrieverbände zeigten sich besorgt über den Grundsatz der Technologieneutralität, da leitungsgebundene Geräte nicht unter den Rechtsakt fallen. Die Folgenabschätzung bestätigt, dass die drahtlosen Geräte ein höheres Risiko für die Cybersicherheit bergen und daher spezifische politische Maßnahmen für diese Funkanlagen ergriffen werden sollten.
- Ein Branchenverband wies darauf hin, dass nicht alle von Kindern verwendeten Geräte unter den Rechtsakt fielen. In dieser Hinsicht wird der Schutz der Privatsphäre von Kindern durch die Verpflichtungen gewährleistet, die Herstellern von mit dem Internet verbundenen Geräten, Spielzeug und Kinderbetreuungsgeräten auferlegt werden (die beiden letzten, auch wenn sie nicht in der Lage sind, über das Internet zu kommunizieren). Von Kindern verwendete Funkanlagen gehören weitgehend zu den oben genannten Kategorien.
- Schließlich zeigte sich die Mehrheit der Interessenträger besorgt über den Übergangszeitraum, der als zu kurz oder zu lang angesehen wird. Es wird davon ausgegangen, dass der Übergangszeitraum von 30 Monaten das richtige Gleichgewicht zwischen der Notwendigkeit, die Cybersicherheit der Funkanlagen auf dem europäischen Markt dringend zu verbessern, und der Notwendigkeit, Herstellern angemessene Zeit für die Anpassung ihrer Produkte einzuräumen, bietet.

4. RECHTLICHE ASPEKTE DES DELEGIERTEN RECHTSAKTS

Das Ziel der vorliegenden Delegierten Verordnung ist es, die in Artikel 3 Absatz 3 Buchstaben d, e und f[17] der Funkanlagenrichtlinie festgelegten grundlegenden Anforderungen, die sich auf Elemente der Cybersicherheit beziehen, auf die Kategorien von Funkanlagen anwendbar werden, die Risiken für die Cybersicherheit darstellen.

[17] d) Schutz des Netzes, e) Schutz personenbezogener Daten und der Privatsphäre sowie f) Schutz vor Betrug.

Konkret ist darin vorgesehen, dass Artikel 3 Absatz 3 Buchstaben d, e und f der Funkanlagenrichtlinie vorbehaltlich bestimmter im Delegierten Rechtsakt genannter Ausnahmen für mit dem Internet verbundene Funkanlagen im Sinne des Artikels 1 gilt.

Darüber hinaus gilt Artikel 3 Absatz 3 Buchstabe e der Funkanlagenrichtlinie vorbehaltlich bestimmter im Delegierten Rechtsakt festgelegter Ausnahmen für tragbare Funkanlagen, für Spielzeug, bei dem es sich auch um Funkanlagen handelt, sowie für Funkanlagen für die Kinderbetreuung, unabhängig davon, ob diese mit dem Internet verbunden sind oder nicht.

Die Delegierte Verordnung steht im Einklang mit den Grundsätzen, die in verschiedenen einschlägigen EU-Rechtsvorschriften festgelegt sind, insbesondere mit den EU-Rechtsvorschriften im Bereich der Cybersicherheit.

Das Datum der Anwendbarkeit der Delegierten Verordnung beträgt 30 Monate ab ihrem Inkrafttreten. Daher wird die Delegierte Verordnung keine Auswirkungen auf Funkanlagen haben, die vor diesem Zeitpunkt der Anwendbarkeit in der Union in Verkehr gebracht wurden.

Die Delegierte Verordnung hat keine Auswirkungen auf den EU-Haushalt.

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 29.10.2021

zur Ergänzung der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, auf die in Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie Bezug genommen wird

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG,[1] insbesondere auf Artikel 3 Absatz 3 zweiter Unterabsatz Buchstaben d, e und f in Verbindung mit Artikel 3 Absatz 3 erster Unterabsatz,

in Erwägung nachstehender Gründe:

(1) Der Schutz des Netzes oder seines Betriebs vor Schaden, der Schutz personenbezogener Daten und der Privatsphäre des Nutzers und des Teilnehmers sowie der Schutz vor Betrug sind Elemente, die den Schutz vor Risiken für die Cybersicherheit unterstützen.

(2) Wie in Erwägungsgrund 13 der Richtlinie 2014/53/EU ausgeführt, können der Schutz personenbezogener Daten und der Privatsphäre der Nutzer von und Teilnehmer an Funkanlagen sowie der Schutz vor Betrug durch besondere Funktionen der Anlagen verbessert werden. Nach diesem Erwägungsgrund sollten Funkanlagen daher im geeigneten Fall so konzipiert sein, dass sie diese Funktionen unterstützen.

(3) 5G wird in den kommenden Jahren eine Schlüsselrolle bei der Entwicklung der digitalen Wirtschaft und Gesellschaft der Union spielen und sich potenziell auf fast alle Aspekte des Lebens der Unionsbürgerinnen und -bürger auswirken. Im Dokument „EU-Instrumentarium für die 5G-Cybersicherheit“[2] wird eine Reihe möglicher gemeinsamer Maßnahmen identifiziert, mit denen die größten Risiken für die Cybersicherheit von 5G-Netzen gemindert werden können, und es bietet eine Orientierungshilfe bei der Auswahl von Maßnahmen, die in den nationalen und EU-Risikominderungsplänen priorisiert werden sollten. Zusätzlich zu diesen Maßnahmen ist es sehr wichtig, einen harmonisierten Ansatz für die grundlegenden Anforderungen in Bezug auf Elemente der Bewahrung der Cybersicherheit zu verfolgen, die für 5G-Funkgeräte gelten sollen, wenn diese auf dem Unionsmarkt in Verkehr gebracht werden.

[1] ABl. L 153 vom 22.5.2014, S. 62.

[2] EU-Instrumentarium für die 5G-Cybersicherheit, 29. Januar 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

(4) Das nach den grundlegenden Anforderungen der Union gemäß Artikel 3 Absatz 3 Buchstaben d, e und f geltende Sicherheitsniveau zur Gewährleistung des Schutzes des Netzes, der Sicherheitsvorrichtungen für den Schutz personenbezogener Daten und der Privatsphäre sowie des Schutzes vor Betrug darf das auf nationaler Ebene geforderte hohe Sicherheitsniveau für dezentrale intelligente Netze im Energiebereich, wo intelligente Zähler verwendet werden sollen, die diesen Anforderungen unterliegen, und für 5G-Netzgeräte, die von Anbietern öffentlicher elektronischer Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972 verwendet werden, nicht beeinträchtigen.

(5) Zahlreiche Bedenken wurden auch in Bezug auf die zunehmenden Risiken für die Cybersicherheit geäußert, die sich daraus ergeben, dass Fachleute und Verbraucher, darunter auch Kinder, zunehmend Funkanlagen nutzen, die: i) selbst in der Lage sind, über das Internet zu kommunizieren, unabhängig davon, ob sie direkt oder über ein anderes Gerät kommunizieren („mit dem Internet verbundene Funkanlagen"), d. h. solche mit dem Internet verbundene Geräte arbeiten mit Protokollen, die für den Datenaustausch mit dem Internet entweder direkt oder über ein Zwischengerät erforderlich sind; ii) entweder Spielzeuge mit Funkfunktion sind, die auch in den Anwendungsbereich der Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates[3] fallen, oder ausschließlich für die Kinderbetreuung konzipiert oder bestimmt sind, wie z. B. Babyfone; oder iii) ausschließlich oder nicht ausschließlich dazu konzipiert oder bestimmt sind, an einem Teil des menschlichen Körpers (einschließlich Kopf, Hals, Rumpf, Arme, Hände, Beine und Füße) oder an von Menschen getragenen Kleidungsstücken (einschließlich Kopfbedeckungen, Handschuhen und Schuhen) getragen, festgeschnallt oder befestigt zu werden, wie z. B. Funkanlagen in Form einer Armbanduhr, eines Rings, eines Armbands, eines Headsets, eines Kopfhörers oder einer Brille („tragbare Funkanlagen").

(6) In diesem Zusammenhang sollten Funkanlagen für die Kinderbetreuung, Funkanlagen, die unter die Richtlinie 2009/48/EG fallen, oder tragbare Funkanlagen, die selbst in der Lage sind, über das Internet zu kommunizieren, unabhängig davon, ob sie direkt oder über ein anderes Gerät kommunizieren, als mit dem Internet verbundene Funkanlagen gelten. Implantate sollten beispielsweise nicht als tragbare Funkanlagen gelten, da sie weder am Körper noch an der Kleidung getragen, festgeschnallt oder befestigt werden. Implantate sollten jedoch als mit dem Internet verbundene Funkanlagen gelten, wenn sie selbst in der Lage sind, über das Internet zu kommunizieren, unabhängig davon, ob sie direkt oder über ein anderes Gerät kommunizieren.

(7) Angesichts der Bedenken aufgrund der Tatsache, dass Funkanlagen keinen Schutz vor Risikoelementen für die Cybersicherheit bieten, ist es erforderlich, auf Funkanlagen bestimmter Kategorien oder Klassen die grundlegenden Anforderungen der Richtlinie 2014/53/EU in Bezug auf den Schutz des Netzes vor Schaden, den Schutz personenbezogener Daten und der Privatsphäre des Nutzers und des Teilnehmers sowie den Schutz vor Betrug anzuwenden.

(8) Die Richtlinie 2014/53/EU gilt für Produkte, die der Definition des Begriffs „Funkanlagen" in Artikel 2 entsprechen, vorbehaltlich besonderer Ausnahmen gemäß Artikel 1 Absatz 2 und Artikel 1 Absatz 3. Während sich die Definition von

[3] Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug (ABl. L 170 vom 30.6.2009, S. 1).

Funkanlagen in Artikel 2 der Richtlinie 2014/53/EU auf Anlagen bezieht, die per Funkwellen kommunizieren können, wird in den Anforderungen der Richtlinie 2014/53/EU nicht zwischen den funkbasierten und nicht funkbasierten Funktionen der Funkanlage unterschieden; daher sollten alle Aspekte und Teile der Anlage die in dieser Delegierten Verordnung vorgesehenen grundlegenden Anforderungen erfüllen.

(9) Was die schädlichen Auswirkungen auf das Netz oder seinen Betrieb oder eine missbräuchliche Nutzung von Netzressourcen betrifft, so kann eine unannehmbare Beeinträchtigung des Dienstes durch mit dem Internet verbundene Funkanlagen verursacht werden, von denen nicht gewährleistet wird, dass Netze keinen Schaden erleiden oder missbraucht werden. Beispielsweise kann ein Angreifer eine mutwillige Überlastung der Netzinfrastruktur herbeiführen, um den regulären Netzverkehr zu behindern, die Verbindungen zwischen zwei Funkprodukten stören und so den Zugang zu einem Dienst verhindern, eine bestimmte Person am Zugang zu einem Dienst hindern, einen Dienst für ein bestimmtes System oder eine bestimmte Person unterbrechen oder den Informationsfluss stören. Die Beeinträchtigung der Online-Dienste kann somit zu böswilligen Cyberangriffen führen, die mit höheren Kosten, Unannehmlichkeiten oder Risiken für Betreiber, Diensteanbieter oder Nutzer verbunden sind. Die Anforderung aus Artikel 3 Absatz 3 Buchstabe d der Richtlinie 2014/53/EU, dass Funkanlagen weder schädliche Auswirkungen auf das Netz oder seinen Betrieb haben noch eine missbräuchliche Nutzung von Netzressourcen ermöglichen, die eine unannehmbare Beeinträchtigung des Dienstes verursachen würde, sollte daher für mit dem Internet verbundene Funkanlagen gelten.

(10) Bedenken wurden auch hinsichtlich des Schutzes personenbezogener Daten und der Privatsphäre des Nutzers und des Teilnehmers von mit dem Internet verbundenen Funkanlagen geäußert, da diese Funkanlagen in der Lage sind, Informationen aufzuzeichnen, zu speichern und weiterzugeben und mit dem Nutzer, auch Kindern, zu interagieren, wenn Lautsprecher, Mikrofone und andere Sensoren in diese Funkanlage integriert sind. Diese Bedenken beziehen sich besonders auf die Fähigkeit dieser Funkanlagen, Fotos, Videos, Lokalisierungsdaten, Daten im Zusammenhang mit der Spielerfahrung sowie die Herzfrequenz, Schlafgewohnheiten oder andere personenbezogene Daten aufzuzeichnen. So kann beispielsweise über ein Standardpasswort auf erweiterte Einstellungen des Funkgeräts zugegriffen werden, wenn die Verbindung oder die Daten nicht verschlüsselt sind oder wenn es keinen starken Authentifizierungsmechanismus gibt.

(11) Daher ist es wichtig, dass mit dem Internet verbundene Funkanlagen, die auf dem Unionsmarkt in Verkehr gebracht werden, sofern sie personenbezogene Daten im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) 2016/679[4] oder Daten im Sinne von Artikel 2 Buchstaben b und c der Richtlinie 2002/58/EG[5] verarbeiten können, über Sicherheitsvorrichtungen verfügen, die gewährleisten, dass personenbezogene

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[5] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Daten und die Privatsphäre geschützt werden. Artikel 3 Absatz 3 Buchstabe e der Richtlinie 2014/53/EU sollte daher für mit dem Internet verbundene Funkanlagen gelten.

(12) Darüber hinaus stellen Funkanlagen für die Kinderbetreuung, Funkanlagen, die unter den Anwendungsbereich der Richtlinie 2009/48/EG fallen, sowie tragbare Funkanlagen hinsichtlich des Schutzes personenbezogener Daten und der Privatsphäre auch ohne Verbindung mit dem Internet Sicherheitsrisiken dar. Personenbezogene Daten können abgefangen werden, wenn Funkanlagen Funkwellen ausstrahlen oder empfangen und über keine Sicherheitsvorrichtungen verfügen, die den Schutz personenbezogener Daten und den Schutz der Privatsphäre gewährleisten. Funkanlagen für die Kinderbetreuung, Funkanlagen, die unter den Anwendungsbereich der Richtlinie 2009/48/EG fallen, sowie tragbare Funkanlagen können mit der Zeit eine Reihe sensibler (personenbezogener) Daten des Nutzers beobachten und speichern und sie über möglicherweise unsichere Kommunikationstechnologien weiterleiten. Funkanlagen für die Kinderbetreuung, Funkanlagen, die unter den Anwendungsbereich der Richtlinie 2009/48/EG fallen, sowie tragbare Funkanlagen sollten auch den Schutz personenbezogener Daten und der Privatsphäre gewährleisten, wenn sie gemäß Artikel 4 Absatz 2 der Verordnung (EU) 2016/679 personenbezogene Daten im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) 2016/679 oder Verkehrsdaten und Standortdaten im Sinne von Artikel 2 Buchstaben b und c der Richtlinie 2002/58/EG verarbeiten können. Artikel 3 Absatz 3 Buchstabe e der Richtlinie 2014/53/EU sollte daher für diese Funkanlagen gelten.

(13) Was Betrug betrifft, können Informationen, einschließlich personenbezogener Daten, aus mit dem Internet verbundenen Funkanlagen gestohlen werden, die keinen Schutz vor Betrug bieten. Bestimmte Arten von Betrug betreffen mit dem Internet verbundene Funkanlagen, wenn sie für Zahlungen über das Internet verwendet werden. Damit können nicht nur auf die Person, die den Betrug erlitten hat, sondern auch auf die Gesellschaft als Ganzes hohe Kosten (z. B. Kosten für polizeiliche Ermittlungen, für Opferdienste oder Prozesskosten zur Feststellung der Verantwortlichen) zukommen. Es ist daher notwendig, vertrauenswürdige Transaktionen zu gewährleisten und das Risiko von finanziellen Verlusten für die Nutzer von mit dem Internet verbundenen Funkanlagen, die Zahlungen über diese Funkanlage ausführen, und die Empfänger der über diese Funkanlage geleisteten Zahlungen zu minimieren.

(14) Mit dem Internet verbundene Funkanlagen, die auf dem Unionsmarkt in Verkehr gebracht werden, sollten im Fall, dass sie dem Besitzer oder Nutzer ermöglichen, Geld, monetäre Werte oder virtuelle Währungen im Sinne von Artikel 2 Buchstabe d der Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates[6] zu übertragen, Funktionen zum Schutz vor Betrug unterstützen. Artikel 3 Absatz 3 Buchstabe f der Richtlinie 2014/53/EU sollte daher für diese Funkanlagen gelten.

(15) Die Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates[7] enthält Vorschriften für Medizinprodukte und die Verordnung (EU) 2017/746 des

[6] Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates (ABl. L 123 vom 10.5.2019, S. 18).

[7] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1).

Europäischen Parlaments und des Rates[8] enthält Vorschriften für In-vitro-Diagnostika. Sowohl in der Verordnung (EU) 2017/745 als auch in der Verordnung (EU) 2017/746 werden bestimmte Aspekte der Risiken für die Cybersicherheit behandelt, die mit den in Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie 2014/53/EU genannten Risiken verbunden sind. Funkanlagen, auf die eine dieser Verordnungen Anwendung findet, sollten daher nicht unter die Kategorien oder Klassen von Funkanlagen fallen, die den grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie 2014/53/EU entsprechen sollten.

(16) Die Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates[9] legt die Anforderungen für die Typgenehmigung von Kraftfahrzeugen sowie von Systemen und Bauteilen für diese Fahrzeuge fest. Außerdem besteht das Hauptziel der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates[10] in der Festlegung und Aufrechterhaltung eines hohen einheitlichen Niveaus der Flugsicherheit in der Union. Des Weiteren sind in der Richtlinie (EU) 2019/520 des Europäischen Parlaments und des Rates[11] die Bedingungen für die Interoperabilität elektronischer Mautsysteme und die Erleichterung des grenzüberschreitenden Informationsaustauschs über die Nichtzahlung von Straßenbenutzungsgebühren in der Union festgelegt. In den Verordnungen (EU) 2019/2144 und (EU) 2018/1139 sowie in der Richtlinie (EU) 2019/520 werden Aspekte von Risiken für die Cybersicherheit behandelt, die mit den in Artikel 3 Absatz 3 Buchstaben e und f der Richtlinie 2014/53/EU genannten Risiken verbunden sind. Funkanlagen, für die die Verordnungen (EU) 2019/2144 und (EU) 2018/1139 oder die Richtlinie (EU) 2019/520 gelten, sollten daher nicht unter die Kategorien oder Klassen von Funkanlagen fallen, die den grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben e und f der Richtlinie 2014/53/EU entsprechen sollten.

(17) In Artikel 3 der Richtlinie 2014/53/EU sind grundlegende Anforderungen, die die Wirtschaftsakteure erfüllen müssen, festgelegt. Um die Konformitätsbewertung in Bezug auf diese Anforderungen zu erleichtern, ist darin eine Konformitätsvermutung für Funkanlagen vorgesehen, die den freiwilligen harmonisierten Normen entspricht,

---

[8] Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176).

[9] Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission (ABl. L 325 vom 16.12.2019, S. 1).

[10] Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1).

[11] Richtlinie (EU) 2019/520 des Europäischen Parlaments und des Rates vom 19. März 2019 über die Interoperabilität elektronischer Mautsysteme und die Erleichterung des grenzüberschreitenden Informationsaustauschs über die Nichtzahlung von Straßenbenutzungsgebühren in der Union (ABl. L 91 vom 29.3.2019, S. 45).

die nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[12] für die Festlegung genauer technischer Spezifikationen zu diesen Anforderungen angenommen werden. In den Spezifikationen würde das auf die bestimmungsgemäße Verwendung der einzelnen von dieser Verordnung betroffenen Kategorien oder Klassen von Funkanlagen bezogene Risikoniveau berücksichtigt und behandelt.

(18) Den Wirtschaftsakteuren sollte ausreichend Zeit für die Anpassung an die Anforderungen dieser Verordnung eingeräumt werden. Diese Verordnung sollte daher erst nach einer gewissen Zeit in Kraft treten und sollte eine Einhaltung ab dem Zeitpunkt ihres Inkrafttretens durch die Wirtschaftsteilnehmer nicht behindern.

(19) Die Kommission hat bei den vorbereitenden Arbeiten zu den Maßnahmen, wie sie in dieser Verordnung festgelegt sind, angemessene Konsultationen durchgeführt und die Sachverständigengruppe für Funkanlagen konsultiert —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

(1) Die grundlegende Anforderung nach Artikel 3 Absatz 3 Buchstabe d der Richtlinie 2014/53/EU gilt für alle Funkanlagen, die selbst über das Internet kommunizieren können, unabhängig davon, ob sie direkt oder über andere Geräte kommunizieren („mit dem Internet verbundene Funkanlagen“).

(2) Die grundlegende Anforderung nach Artikel 3 Absatz 3 Buchstabe e der Richtlinie 2014/53/EU gilt für die folgenden Funkanlagen, sofern diese Funkanlagen im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) 2016/679 personenbezogene Daten im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) 2016/679 oder Verkehrsdaten und Standortdaten im Sinne von Artikel 2 Buchstaben b und c der Richtlinie 2002/58/EG verarbeiten können:

(a) mit dem Internet verbundene Funkanlagen, die nicht unter den Buchstaben b, c oder d genannt sind,

(b) Funkanlagen, die ausschließlich für die Kinderbetreuung konzipiert oder bestimmt sind,

(c) Funkanlagen, die unter die Richtlinie 2009/48/EG fallen,

(d) Funkanlagen, die ausschließlich oder nicht ausschließlich dazu konzipiert oder bestimmt sind, an Folgendem getragen, festgeschnallt oder befestigt zu werden:

(i) einem Teil des menschlichen Körpers, einschließlich Kopf, Hals, Rumpf, Arme, Hände, Beine und Füße,

(ii) oder an von Menschen getragenen Kleidungsstücken, einschließlich Kopfbedeckungen, Handschuhen und Schuhen.

[12] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

(3) Die grundlegende Anforderung nach Artikel 3 Absatz 3 Buchstabe f der Richtlinie 2014/53/EU gilt für alle mit dem Internet verbundenen Funkanlagen, wenn diese dem Besitzer oder Nutzer ermöglichen, Geld, monetäre Werte oder virtuelle Währungen im Sinne von Artikel 2 Buchstabe d der Richtlinie (EU) 2019/713 zu übertragen.

Artikel 2

(1) Abweichend von Artikel 1 gelten die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie 2014/53/EU nicht für Funkanlagen, für die auch eine der folgenden Rechtsvorschriften der Union gilt:

(a) Verordnung (EU) 2017/745,

(b) Verordnung (EU) 2017/746.

(2) Abweichend von Artikel 1 Absatz 2 und Artikel 1 Absatz 3 gelten die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben e und f der Richtlinie 2014/53/EU nicht für Funkanlagen, für die auch eine der folgenden Rechtsvorschriften der Union gilt:

(a) Verordnung (EU) 2018/1139,

(b) Verordnung (EU) 2019/2144,

(c) Richtlinie (EU) 2019/520.

Artikel 3

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem … [*Amt für Veröffentlichung: Bitte Datum einfügen: 30 Monate nach dem Datum des Inkrafttretens dieser Verordnung*].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 29.10.2021

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN