Deutscher Bundestag **Drucksache 19/18649**

19. Wahlperiode 17.04.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller und der Fraktion der AfD
– Drucksache 19/18023 –

Förderung von IT-Sicherheit und IT-Souveränität durch den Bund

Vorbemerkung der Fragesteller

Nach einer „durchwachsenen“ Gesamtbilanz der Digitalen Agenda 2014–2017 (https://www.zdf.de/nachrichten/heute-journal/digitale-agenda-durchwachsene-bilanz-100.html; https://www.zdf.de/politik/berlin-direkt/zypries-fazit-digitale-agenda-100.html) und dem gebrochenen Versprechen von Bundeskanzlerin Dr. Angela Merkel hinsichtlich des Ausbaus der digitalen Infrastruktur (https://www.pcwelt.de/news/Bundesregierung-bricht-Versprechen-bei-Breitbandausbau-10612139.html) wurde im Rahmen der im November 2018 verabschiedeten Digitalstrategie der Bundesregierung ein Maßnahmenpaket entwickelt und in einer Umsetzungsstrategie zusammengefasst (https://www.bundesregierung.de/resource/blob/992814/1605036/61c3db982d81ec0b4698548fd19e52f1/digitalisierung-gestalten-download-bpa-data.pdf?download=1), von der mittlerweile mindestens drei Versionen vorliegen mit jeweils mehreren überarbeiteten Auflagen.

In dieser Umsetzungsstrategie werden einzelne Vorhaben und die jeweils verantwortlichen Ressorts benannt, jedoch sind nur teilweise konkrete Zeitpläne für Beginn und Zielerreichung angegeben. Die zur Verfügung stehenden Ressourcen zur Zielerreichung werden ebenso wenig genannt wie eine Priorisierung von Vorhaben.

Maßnahmen zur Förderung von IT-Sicherheit und IT-Souveränität sind über sieben Bundesministerien verteilt.

1. Wie viele Transfers neuer IT-Sicherheitskonzepte für Industrie 4.0 in die wirtschaftliche Anwendung im Mittelstand sind im Nationalen Referenzprojekt „IUNO“ (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 81) bislang erfolgt?

   a) Wie viele transferierte Konzepte und wie viele anwendende Unternehmen werden angestrebt, um den Titel eines Nationalen Referenzprojektes zu rechtfertigen?

Das inzwischen abgeschlossene Referenzprojekt IUNO hatte zum Ziel, Referenzkonzepte zu entwickeln, die Unternehmen zur Entwicklung spezifischer

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Wirtschaft und Energie vom 15. April 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

IT-Sicherheitslösungen zur Verfügung stehen. Der Transfer war nicht Aufgabe des nationalen Referenzprojektes IUNO; hierfür wurde im Nachgang das Transferprojekt IUNO-Insec gestartet.

b) Bis wann soll dieses Transferziel erreicht werden, damit die entwickelten Lösungen nicht bereits wieder veraltet sind?

Die Transfer- und Umsetzungsprojekte in IUNO-Insec laufen planmäßig bis Mai 2022. Dem Problem des Veraltens wurde im Nationalen Referenzprojekt zur IT-Sicherheit in der Industrie 4.0 konzeptionell begegnet, indem generische Referenzbausteine entwickelt wurden. Diese haben gerade die Eigenschaft, dass sie langfristig anwendbar sind und nicht von kurzlebigen Trends abhängen.

2. Wurde das in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ im März 2019 angekündigte „Pilotnetz“ im Rahmen des Förderschwerpunktes des Bundesministeriums für Bildung und Forschung „Anwendungsszenarien der Quantenkommunikation“ (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 81) zur Erprobung des Transfers in die Anwendung bereits fertiggestellt?

a) Wenn nein, warum nicht, und mit welchen anderen Instrumenten soll der Transfer in die Anwendung „frühzeitig“ erprobt werden?

c) Liegen bereits Zwischenberichte zur Arbeit des Pilotnetzes vor?

Das im März 2019 angekündigte Projekt zur Erprobung der Quantenkommunikation wurde im vierten Quartal 2019 gestartet und läuft derzeit. Dementsprechend liegen noch keine Zwischenberichte vor. Dieses Projekt ist das Instrument zur frühzeitigen Erprobung eines Transfers dieser Schlüsseltechnologie in die Anwendung.

b) Welche Beteiligte umfasst das Pilotnetz, und wie wurden diese ausgewählt?

Beteiligt sind die Fraunhofer-Gesellschaft, die Max-Planck-Gesellschaft und das Deutsche Zentrum für Luft- und Raumfahrt. Das Konsortium bündelt die notwendigen Kompetenzen, um das wichtige forschungspolitische Ziel, eine Quantenkommunikationsinfrastruktur zu realisieren, umzusetzen. Bedarfsorientiert werden weitere Partner aus Wissenschaft und Wirtschaft eingebunden. Die Federführung für dieses auf den Transfer in die Anwendung ausgelegte Großprojekt hat das Bundesministerium für Bildung und Forschung in die Hände der Fraunhofer-Gesellschaft gelegt.

3. Wie viele Krankenhäuser mit mindestens 30.000 vollstationären Fällen im Jahr, die damit als kritische Infrastruktur (KRITIS) gelten, haben pflichtgemäß auf Basis des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zum 30. Juni 2019 nach Kenntnis der Bundesregierung organisatorische und technische Vorkehrungen getroffen, um ihre IT-Systeme auf den Stand der Technik zu bringen und haben dies bereits dem Bundesamt für Sicherheit in der Informationstechnik nachgewiesen (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 35)?

132 Krankenhäuser in Deutschland sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als KRITIS im Sinne des BSI-Gesetzes (BSIG) registriert. Eine Unterteilung nach vollstationären Fällen im Jahr erfolgt seitens

des BSI dabei nicht. Alle beim BSI registrierten KRITIS-Betreiber haben pflichtgemäß organisatorische und technische Vorkehrungen getroffen, um ihre IT-Systeme auf den Stand der Technik zu bringen. Der Großteil hat dies bereits dem BSI nachgewiesen. Lediglich 10 Krankenhäuser haben ihren Nachweisprozess noch nicht abgeschlossen und dem BSI noch keine entsprechenden Unterlagen zur Verfügung gestellt. Das BSI ist im engen Austausch mit diesen Betreibern und begleitet den Prozess.

Das BSIG belässt das Ableiten von konkreten Maßnahmen zur Erfüllung des § 8a Absatz 1 BSIG in der Verantwortung der KRITIS-Betreiber. Dies ist aus Sicht des BSI auch sinnvoll, da nur so sichergestellt ist, dass die Maßnahmen passgenau und angemessen sind. Zur Konkretisierung der zu ergreifenden Maßnahmen und umzusetzenden Anforderungen sieht das BSIG das Werkzeug der „Branchenspezifischen Sicherheitsstandards“ (B3S) vor. Diese werden von Betreibern vorgeschlagen und vom BSI auf Eignung geprüft.

a) Bis wann wurden die konkreten Anforderungen, die mit diesen Vorkehrungen verbunden sind, von den entsprechenden Fachkreisen mit dem BSI abgestimmt, und wann wurden die finalen Anforderungen verabschiedet?

Die Deutsche Krankenhausgesellschaft (DKG) hatte nach erfolgter Abstimmung und Freigabe durch den Branchenarbeitskreis „Medizinische Versorgung“ des UP KRITIS und die zuständigen Gremien der DKG dem BSI am 18. Dezember 2018 einen finalisierten Entwurf eines B3S mit der Bitte um Feststellung der Eignung übersendet. Nach einem weiteren Abstimmungsprozess erfolgte am 19. August 2019 die Feststellung der Eignung der finalen Fassung (Version 1.1) durch das BSI.

b) Welche Investitionen in die IT-Ausstattung und in erforderliche bauliche Maßnahmen wurden in welcher Höhe aus Mitteln des Krankenhausstrukturfonds gefördert?

Bisher sind noch keine Investitionen zur Verbesserung der informationstechnischen Sicherheit von Krankenhäusern aus Mitteln des Krankenhausstrukturfonds gefördert worden.

c) Gibt es für diese KRITIS-Krankenhäuser weitere Förderungen oder Unterstützungen durch den Bund, und wenn ja, welche, bis wann, und unter welchen Auflagen?

Aus Mitteln des Krankenhausstrukturfonds können Maßnahmen zur Verbesserung der IT-Sicherheit bei Krankenhäusern gefördert werden, die als Kritische Infrastruktur gelten mit Ausnahme der Hochschulkliniken. Gefördert werden können die Kosten für die Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer Anlagen, Systeme oder Verfahren oder bauliche Maßnahmen, die erforderlich sind, um die Informationstechnik der betroffenen Krankenhäuser an die Vorgaben des § 8a BSIG anzupassen. Für bauliche Maßnahmen dürfen dabei nur 10 Prozent der beantragten Fördermittel verwendet werden. Auf Grund dieser umfassenden Förderung sind weitere Förderungen oder Unterstützungen der betroffenen Krankenhäuser durch den Bund nicht erforderlich, damit diese den gesetzlich vorgegebenen Stand der IT-Sicherheit erreichen können.

d) Um welche „Rechtssetzungsmaßnahme“ (ebenda, S. 35) handelt es sich, die in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ als Umsetzungsschritt zur Förderung von Investitionen in IT-Sicherheit für Krankenhäuser, die als kritische Infrastruktur identifiziert wurden, angekündigt wurde?

Bei den erwähnten Rechtssetzungsmaßnahmen handelt es sich um § 12a des Krankenhausfinanzierungsgesetzes und um die §§ 11 ff. der Krankenhausstrukturfonds-Verordnung.

4. Beabsichtigt die Bundesregierung, auch Investitionen in die IT-Ausstattung und in bauliche Maßnahmen durch Arztpraxen und Zahnarztpraxen finanziell zu fördern, die durch die künftige Umsetzung des Digitale-Versorgung-Gesetzes und der Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung ab Juni 2020 erforderlich werden (Antwort der Bundesregierung auf Bundestagsdrucksache 19/15031 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14556, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten‘ – Maßnahmen zur Erhöhung der IT-Sicherheit für Leistungserbringer, die nicht von der BSI-Kritisverordnung erfasst werden“)?

Die Bundesregierung beabsichtigt keine finanzielle Förderung.

a) Wenn nein, warum nicht?

b) Wenn ja, bis zu welcher Höhe je Arztpraxis und Zahnarztpraxis?

Wie aus der Einschätzung des Erfüllungsaufwandes (vgl. Bundestagsdrucksache 19/13438), bestätigt durch den Nationalen Normenkontrollrat (vgl. Bundestagsdrucksache 19/14867), folgt, besteht weder die Notwendigkeit, bauliche Veränderungen noch Veränderungen an der IT-Ausstattung vorzunehmen. Da keine zusätzlichen Aufwände begründet werden, bedarf es keiner gesonderten finanziellen Förderung.

c) Welche weitere Unterstützung organisatorischer, technischer, personeller oder sonstiger Natur beabsichtigt die Bundesregierung?

Die Bundesregierung bewertet laufend die Wirkungen umgesetzter Maßnahmen. Dies umfasst auch die mit dem Digitale-Versorgung-Gesetz eingeführten Vorgaben. Daher sind über die in § 75b des Fünften Buches Sozialgesetzbuch (SGB V) formulierten Anforderungen hinaus derzeit keine weiteren Maßnahmen geplant.

d) In welcher Form ist die Bundesregierung in die derzeit laufende Erarbeitung der Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung durch die Kassenärztliche Bundesvereinigung und die Kassenzahnärztliche Bundesvereinigung eingebunden (ebenda), und wie kann sie eine Fertigstellung der Richtlinie bis zum Juni 2020 gewährleisten?

Gemäß § 75b Absatz 1 Satz 1 SGB V liegt die Zuständigkeit für die Erstellung der Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung bei den Kassenärztlichen Bundesvereinigungen. Gemäß § 75b Absatz 3 Satz 2 und 3 erfolgt die Erstellung im Einvernehmen mit dem BSI und im Benehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Gesellschaft für Telematik, der Bundesärztekammer, der Bundeszahnärztekammer, der DKG und den für die Wahrnehmung

der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen.

Daher ist die Bundesregierung ganz aktuell im Rahmen der Einvernehmenserstellung mit dem BSI in die Erarbeitung der Richtlinie involviert. Im Übrigen wird zum gegenwärtigen Zeitpunkt von einer fristgemäßen Erarbeitung der Richtlinie ausgegangen.

5. Wie viele KMU-Projekte (KMU = kleine und mittlere Unternehmen) wurden bislang im Rahmen der Ende 2018 veröffentlichten Förderbekanntmachung zur IT-Sicherheit in der Wirtschaft, wie in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ angekündigt (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 63), durch das federführende Bundesministerium für Wirtschaft und Energie (BMWi) bewilligt?

Seit der Veröffentlichung der Förderbekanntmachung wurden drei Projekte bewilligt und werden derzeit umgesetzt. Sieben weitere Vorhaben befinden sich in der Phase der Antragstellung/-prüfung.

a) Wie viele KMU-Projekte sollen insgesamt im Rahmen der Förderbekanntmachung zur IT-Sicherheit bewilligt werden?

Die Bewilligung ist abhängig von den zur Verfügung stehenden Haushaltsmittel und den beantragten Projektvolumen. Ziel ist es nicht, möglichst viele Projekte umzusetzen, sondern erfolgreiche Maßnahmen mit einem bestmöglichen Nutzen für KMU, um konkrete Unterstützungs-, Sensibilisierungs- und Qualifikationsangebote zur Verfügung zu stellen und in die Breite transferieren zu können.

b) Wurde die Transferstelle „IT-Sicherheit in der Wirtschaft“, wie in der Antwort der Bundesregierung auf Bundestagsdrucksache 19/14791 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14205, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten‘ – Unterstützung des Mittelstands bei der digitalen Transformation“ für „Ende 2019“ angekündigt, bereits eingerichtet, wenn nein, warum nicht?

Die Transferstelle ist zum 1. Januar 2020 bewilligt worden und gestartet. Sie wird durch ein Konsortium bestehend aus Deutschland sicher im Netz (DsiN, Konsortialführer), dem DIHK, dem Kompetenzzentrum für Informationssicherheit der Hochschule Mannheim sowie der Fraunhofer Gesellschaft IAO und FOKUS betrieben. Derzeit befinden sich Transfer- und Demonstrationsangebote inklusive Webpräsenz/Konzept für die Öffentlichkeitsarbeit und Evaluation im Aufbau bzw. in der Abstimmung. Die ersten Angebote sowie die Webpräsenz starten in Kürze.

c) Welche Gründe haben zu der bisher schon existierenden Verzögerung der Einrichtung der Transferstelle geführt, da diese in der September-2019-Version der Umsetzungsstrategie bereits für „Herbst 2019“ angekündigt war (https://www.bundesregierung.de/resource/blob/975292/1605036/61c3db982d81ec0b4698548fd19e52f1/digitalisierung-gestalten-download-bpa-data.pdf?download=1, S. 83)?

Ursächlich für die Verzögerung waren interne Abstimmungsprozesse.

d) Sind weitere Maßnahmen zur praxisnahen Aufbereitung von Unterstützungsangeboten sowie unternehmensnahe Handlungsanleitungen zu mehr IT-Sicherheit des BMWi geplant, und wenn ja, welche?

Im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ werden auch künftig Projekte gefördert, um KMU und Handwerk beim Thema IT-Sicherheit zu sensibilisieren und zu unterstützen mit dem Ziel, das IT-Sicherheitsniveau der Unternehmen zu erhöhen. Weitere praxisnahe Unterstützungsangebote werden von der Transferstelle aufbereitet und auf vielfältige Weise bereitgestellt.

e) Ist die Ausschreibung eines Projektträgers für das neue Förderprogramm „Investitionszuschuss Digitalisierung im Mittelstand“ bereits abgeschlossen, sodass, wie in der Antwort der Bundesregierung auf Bundestagsdrucksache 19/14791 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14205, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten‘ – Unterstützung des Mittelstands bei der digitalen Transformation“ angekündigt, dessen Beauftragung „Anfang 2020“ (ebd.) erfolgen kann?

Das Ausschreibungsverfahren für einen Projektträger für das neue Förderprogramm wird in Kürze abgeschlossen.

f) Welche Gründe haben zu der bisher schon existierenden Verzögerung des Programmstarts geführt, da dieser, und nicht erst die Ausschreibung des Projektträgers, in der November -2018-Version der Umsetzungsstrategie bereits für „Ende 2019“ angekündigt war (https://www.bundesfinanzministerium.de/Content/DE/Downloads/Digitalisierung/2018-11-15-Digitalisierung-gestalten.pdf?__blob=publicationFile&v=2. S. 56)?

Vor der Ausschreibung des Projektträgers mussten die Haushaltsmittel für das Förderprogramm durch den Haushaltsausschuss des Deutschen Bundestages entsperrt werden. Erst danach konnte die Ausschreibung für den Projektträger, der für die Umsetzung des Programms notwendig ist, erfolgen.

g) Wie soll sich der in der Umsetzungsstrategie angekündigte „Fokus auf Investitionen in die IT-Sicherheit“ (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 63) in Höhe und Anteil der Fördersummen ausdrücken?

Für Investitionen im Bereich der IT-Sicherheit, inklusive Datenschutz wird die Förderquote um 5 Prozentpunkte erhöht.

h) In welchem Umfang werden in dem Förderprogramm „go-digital“ KMU bis 100 Mitarbeiter im Programmbereich „IT-Sicherheit“ (ebd.) durch Beratungsleistungen und Umsetzungsleistungen unterstützt?

Seit dem Start der Fördermaßnahme im Sommer 2017 wurden 220 Projekte im Hauptmodul IT-Sicherheit mit einer Fördersumme in Höhe von 1,91 Mio. Euro bewilligt (Stand: 31. März 2020). Darüber hinaus gibt die go-digital-Richtlinie vor, dass in jedem Projekt im Rahmen der beiden anderen Module „Digitalisierung von Geschäftsprozessen“ und „Digitale Markterschließung“ verpflichtend eine „IT-Pflichtberatung“ im Umfang von zwei Beratertagen stattfinden muss.

i) Welche quantitativen und qualitativen Kriterien werden von den Anbietern der Beratungsleistungen und Umsetzungsleistungen zu deren Messung erhoben (bitte diese Kriterien zur Beantwortung der Frage 5i) nutzen)?

Grundsätzlich gilt: Die für das Programm go-digital autorisierten Beratungsunternehmen müssen sich an den Vorgaben des BSI IT-Grundschutz sowie der ISO 27001 orientieren. Zu Beginn der konkreten Beratung fertigt das Beratungsunternehmen eine individuelle, auf das jeweilige KMU zugeschnittene Risiko- und Sicherheitsanalyse seiner IKT-Infrastruktur an. Auf dieser Grundlage kann das Gesamtgefährdungspotential für das begünstigte KMU einschätzt werden. Darauf aufbauend kann das Beratungsunternehmen einen – wiederum – individuellen Maßnahmenkatalog entwickeln, dessen Umsetzung die Integration der allgemein anerkannten Schutzziele wie Vertraulichkeit, Integrität usw. in den betrieblichen Abläufen und Geschäftsprozessen der KMU gewährleistet, wie mit der go-digital-Förderrichtlinie gefordert.

j) Wurden die Anbieter der Beratungsleistungen und Umsetzungsleistungen in den jeweiligen Bewilligungsbescheiden mit Mindestanforderungen hinsichtlich dieser quantitativen und qualitativen Kriterien beauflagt, und wenn nein, warum nicht, und wenn ja, werden die Mindestanforderungen bis zum Ende des Förderzeitraums Ende 2021 nach derzeitigem Planungsstand erfüllt werden?

Wie in der Antwort zu i) ausgeführt, haben die autorisierten Beratungsunternehmen im Beratungsprozess die Vorgaben des BSI IT-Grundschutz und der ISO 27001 zu beachten. Weitere erforderliche Maßnahmen richten sich nach den (im Rahmen der Potenzialanalyse) vorgefundenen individuellen Verhältnissen im Unternehmen. Zum Beratervertrag, der zwischen Beratungsunternehmen und KMU zu schließen ist, gehört schließlich ein Projektplan, der die Anforderungen an die Beratungs- und Umsetzungsleistungen definiert. Dieser ist den Antragsunterlagen beizufügen. Die Bewilligung der Zuwendung kann nur erfolgen, wenn der Projektplan den Anforderungen der go-digital-Förderrichtlinie entspricht.

k) Wie sind die Nutzungsstatistiken zum Digitalisierungsthema „Sicherheit“ auf der zentralen Website www.mittelstand-digital.de, insbesondere des Sicherheitstools Mittelstand (SiToM), z. B. zu den Merkmalen Anzahl Seitenaufrufe, Verweildauer etc.?

Die Inhalte zum Thema IT-Sicherheit auf der Website www.mittelstand-digital.de wurden im Jahr 2019 knapp 3000-mal aufgerufen, mit einer durchschnittlichen Verweildauer von knapp 2 Minuten. Nicht inbegriffen in diese Zahl ist die Nutzung des Sicherheitstools Mittelstand (SiToM), da es für dieses Tool eine eigene Website (www.sitom.de) gibt. Auf dieser Website haben bis zum Stichtag 31. März 2020 bisher knapp 2000 Unternehmen ihr IT-Sicherheitsniveau mit dem SiToM bestimmt. In Kürze startet die Transferstelle mit dem Aufbau einer bundesweiten Transfer- und Unterstützungsinfrastruktur. Über die neuen virtuellen Angebote (mobile App und Webpräsenz) werden KMU Informationen und Maßnahmen zu IT-Sicherheitsthemen vermittelt.

6. Welche Maßnahmen sieht die in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ zur Unterstützung der Umsetzung von Industrie 4.0 beschriebene internationale Kooperationsvereinbarung mit der Volksrepublik China zu den Themen IT- und Cybersicherheit im Einzelnen vor?

   a) Wurde vor Abschluss dieser Vereinbarung mit der Volksrepublik China eine Risikoanalyse zu möglichem Technologieabfluss und Industriespionage durchgeführt?

      Wenn nein, warum nicht, und wenn ja, durch welche Behörde, und mit welchem Ergebnis?

   b) Werden im Rahmen der Kooperationsprojekte zwischen Unternehmen sowie Forschungseinrichtungen nach Kenntnis der Bundesregierung auch Mitarbeiter und Wissenschaftler ausgetauscht, und wenn ja, in welchem Umfang?

   c) Kommt es nach Kenntnis der Bundesregierung lediglich zu einem Austausch vereinzelter Mitarbeiter und Wissenschaftler oder auch zu einem Austausch ganzer Mitarbeitergruppen oder Forschergruppen?

   d) Werden die ausgetauschten chinesischen Mitarbeiter und Wissenschaftler nach Kenntnis der Bundesregierung vorab sicherheitsüberprüft, und wenn nein, warum nicht, und wenn ja, mit welchem Ergebnis?

   e) Wie wird sichergestellt, dass die chinesischen Mitarbeiter und Wissenschaftler nicht im Rahmen des Austausches einer nachrichtendienstlichen Tätigkeit nachgehen oder Industriespionage oder Industriesabotage betreiben?

   f) Wie viele Fälle von Industriespionage oder Industriesabotage oder Technologieabfluss hat es bereits in öffentlich geförderten Projekten, Kooperationen oder sonstigen Formaten mit chinesischer Beteiligung gegeben?

   g) Wie viele Fälle von Industriespionage oder Industriesabotage oder Technologieabfluss betrafen das Themengebiet IT-Sicherheit und Cybersicherheit und Industrie 4.0?

   h) Wurden diese Vorfälle von Industriespionage oder Industriesabotage oder Technologieabfluss bereits adressiert, z. B. im Rahmen der Deutsch-Chinesischen Jahrestagung der Staatssekretäre und Vizeminister im November 2019 in Berlin?

Die Fragen 6 bis 6h werden gemeinsam beantwortet.

In der Kooperation zu Industrie 4.0 mit China werden auch für Industrie 4.0 relevante Themen der Cybersicherheit mit Blick auf Gesetzgebung und Geschäftspraxis diskutiert, da diese großen Einfluss auf die Möglichkeiten und Perspektiven der Umsetzung von Industrie-4.0-Lösungen in China haben. Insgesamt ist es ein Kernziel der Zusammenarbeit, auf eine Verbesserung der Rahmenbedingungen in China für deutsche Unternehmen hinzuwirken. Innerhalb der Industrie-4.0-Kooperation wird kein Technologietransfer vorangetrieben. Allerdings sind sich alle Beteiligten auf deutscher Seite der Problematik von Technologieabfluss und Industriespionage bewusst und berücksichtigen dies laufend bei ihren Beiträgen zur Zusammenarbeit; dies kann in Zukunft auch die Erstellung einer Risikoanalyse bedeuten.

i) Wie bewertet die Bundesregierung den Erfolg des US-chinesischen No-Spy-Abkommens von 2015 (https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/) hinsichtlich einer möglichen Vorbildfunktion für ein deutsch-chinesisches No-Spy-Abkommen?

Der Bundesregierung liegen keine belastbaren Erkenntnisse zu möglichen Erfahrungen aus den USA und China in Bezug auf das in der Frage genannte Abkommen vor.

7. Welche der zahlreichen, teilweise seit März 2017 als „laufend" deklarierten Maßnahmen (https://www.bundesregierung.de/resource/blob/975292/1605036/61c3db982d81ec0b4698548fd19e52f1/digitalisierung-gestalten-download-bpa-data.pdf?download=1, S. 90) zur Förderung der Digitalisierung der Finanzindustrie innerhalb der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten" haben bislang zu Ergebnissen hinsichtlich der angekündigten „Stärkung der Cyber- und IT-Sicherheit im Finanzsektor" (ebd.) geführt?

a) Wie wurde diese „Stärkung der Cyber- und IT-Sicherheit im Finanzsektor" gemessen?

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat in den letzten Jahren die drei Rundschreiben Bankaufsichtliche Anforderungen an die IT (BAIT), Versicherungsaufsichtliche Anforderungen an die IT (VAIT) und Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT) veröffentlicht. Die Einhaltung dieser Anforderungen an die Informationssicherheit und das IT-Risikomanagement von Unternehmen und Instituten des Finanzsektors wird in Form von regelmäßigen IT-Prüfungen überprüft. Außerdem hat Deutschland im letzten Jahr das von der Europäische Zentralbank veröffentlichte Rahmenwerk zur Durchführung von bedrohungsgeleiteten Penetrationstests (TIBER-EU) umgesetzt. Bei der Deutschen Bundesbank können sich Institute und Unternehmen des deutschen Finanzsektors für einen solchen TIBER-Test anmelden.

b) Zu welchen Ergebnissen haben die nationale und internationale Cyberübung im Finanzsektor im September 2018 bzw. im Juni 2019 (Antwort der Bundesregierung auf Bundestagsdrucksache 19/15901 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/15410, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten' – Förderung der Digitalisierung der Finanzindustrie") hinsichtlich der Cybersicherheit und IT-Sicherheit des Finanzsektors sowie des Schutzes und der Integrität von Finanzdaten geführt?

c) Welche Handlungsempfehlungen wurden aus den Ergebnissen der nationalen und internationalen Cyberübung im Finanzsektor im September 2018 bzw. im Juni 2019 hinsichtlich der Cybersicherheit und IT-Sicherheit des Finanzsektors sowie des Schutzes und der Integrität von Finanzdaten abgeleitet?

d) Hat die Bundesregierung bereits mit der Umsetzung möglicher Handlungsempfehlungen aus diesen Übungen begonnen, und wenn nein, warum nicht?

Die Fragen 7b bis 7d werden gemeinsam beantwortet.

Die Nationale Cyberübung im September 2018 diente der nationalen Erprobung der existierenden Melde- und Informationswege zwischen Aufsichtsobjekten und Behörden sowie zwischen den Behörden. Im Ergebnis wurde festgestellt, dass die Melde- und Informationswege funktionieren; Optimierungsmöglichkeiten wurden umgesetzt. Die internationale Cyberübung der G7-Staaten im

Juni diente der Erprobung eines zuvor erarbeiteten G7-Kommunikationsprotokolls der G7-Finanzministerien, -Finanzaufsichtsbehörden und -Zentralbanken sowie der Koordinierung möglicher Maßnahmen anhand eines fiktiven Szenarios. Die Ziele der Übung wurden erreicht und die vorgesehenen Kommunikations-/Informationswege haben sich im Rahmen der Übung als effektiv erwiesen. Die Erarbeitung weiterer Handlungsempfehlungen ist Bestandteil derzeit noch laufender G7-Arbeiten.

e) Aus welchem Grund wurde eine Big Data und Artifical-Intelligence-Studie der Bundesanstalt für Finanzdienstleistungsaufsicht als Umsetzungsschritt der Umsetzungsstrategie „Digitalisierung gestalten“ von November 2018 ausgewiesen, obwohl diese Studie laut Antwort der Bundesregierung auf Bundestagsdrucksache 19/15901 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/ 15410, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten‘ – Förderung der Digitalisierung der Finanzindustrie“, bereits am 15. Juni 2018 und damit vor Verabschiedung der Umsetzungsstrategie, veröffentlicht wurde?

Die Studie der BaFin „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“ ist Ausgangspunkt zahlreicher Maßnahmen, die nach Veröffentlichung der Umsetzungsstrategie stattfanden. An die Veröffentlichung schloss sich eine Konsultations- und eine Auswertungsphase an. Die Ergebnisse dieser Konsultation wurden am 28. Februar 2019 im Rahmen der Schriftenreihe BaFinPerspektiven publiziert (siehe www.bafin.de/dok/120410.3788). Auf der Grundlage der Ergebnisse identifizierte die BaFin Arbeitspakete (Marktanalysen, Aufsicht über algorithmenbasierte Entscheidungsprozesse, Daten und Wettbewerb und Grenzen der Finanzaufsicht untersuchen, BDAI in der Geldwäsche-Erkennung), die sie derzeit bearbeitet.

f) Welche weiteren digitalpolitischen Maßnahmen der Bundesregierung wurden vor November 2018 umgesetzt und wurden dennoch als „Umsetzungsschritt“ der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ deklariert, die im November 2018 veröffentlicht wurde?

Die Umsetzungsstrategie erfasst die Umsetzung digitalpolitischer Schwerpunktvorhaben aller Bundesministerien. Die Erstveröffentlichung der Umsetzungsstrategie im November 2018 definierte dabei nicht den Startpunkt der Vorhaben, die zum Teil vorher begannen oder aus der Digitalen Agenda 2014 – 2017 hervorgingen und weiterentwickelt wurden. Die Fortschritte der Digitalen Agenda 2014 – 2017 sind im Legislaturbericht öffentlich nachzulesen (https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.html). Ein weitergehender Abgleich der Inhalte der Umsetzungsstrategie mit der Digitalen Agenda im Sinne der Fragestellung würden die Arbeitsfähigkeit der betroffenen Bereiche angesichts der aktuellen Belastung durch die Ausbreitung des Coronavirus/Covid-19 unverhältnismäßig einschränken.

g) Wie definiert die Bundesregierung das Instrument „Umsetzungsschritt“ im Rahmen der Umsetzungsstrategie „Digitalisierung gestalten“?

Die Definition eines Umsetzungsschrittes ergibt sich aus dem Wort Umsetzungsschritt selbst. Hiermit ist alles gemeint, was das jeweilige Vorhaben einen Schritt näher an seine Umsetzung bringt.

8. Ist es bereits, wie in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ für 2019/2020 angekündigt (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 82), zu ersten Ideenwettbewerben und Vergaben von gezielten Forschungsaufträgen durch die Agentur für Innovation in der Cybersicherheit gekommen, die den Erhalt von Technologiesouveränität Deutschlands im Cyberraum und Informationsraum sicherstellen soll?

   a) Wenn nein, warum nicht?

   b) Wenn ja, welche konkreten Projektziele verfolgen diese Forschungsaufträge im Einzelnen?

   c) Bis wann ist mit dem Abschluss dieser Forschungsaufträge zu rechnen?

Die Fragen 8 bis 8c werden gemeinsam beantwortet.

Die Agentur für Innovation in der Cybersicherheit GmbH befindet sich aktuell in Gründung. Nachdem im November 2019 durch den Haushaltsausschuss die Errichtung der Agentur in der Rechtsform einer GmbH gebilligt wurde, arbeiten die beiden beteiligten Ressorts, das Bundesministerium des Innern, für Bau und Heimat und das Bundesministerium der Verteidigung, aktuell an den letzten vorbereitenden Schritten zur Gründung.

   d) Wie soll grundsätzlich die in der Wissenschaftssprache „impact“ genannte Wirkung der beauftragten Forschungsaufträge durch die Agentur für Innovation in der Cybersicherheit hinsichtlich des Erhalts von Technologiesouveränität im Cyberraum und Informationsraum gemessen werden?

Die konkrete Ausgestaltung dieser Wirkungsanalyse erfolgt nach Gründung der GmbH in Abstimmung zwischen der Beteiligungsführung und der Geschäftsführung der Agentur. Als eine Möglichkeit wird aktuell das Impact-Maturity-Modell betrachtet.

9. Welche Bereiche, in denen der Einsatz von algorithmenbasierten Systemen für Verbraucher besonders sensibel ist, wurden von der Bundesregierung in der seit November 2018 „laufenden“ Maßnahme „Algorithmenbasierte Entscheidungen überprüfbar machen“ im Rahmen der Umsetzungsstrategie „Digitalisierung gestalten“ wie angekündigt identifiziert (https://www.bundesregierung.de/resource/blob/975292/1605036/61c3db982d81ec0b4698548fd19e52f1/digitalisierung-gestalten-download-bpa-data.pdf?download=1, S. 124)?

Der Einsatz von algorithmischen Systemen birgt neben vielfältigen Chancen für Verbraucherinnen und Verbraucher auch Risiken. Besonders zu prüfen sind beispielsweise Situationen, in denen algorithmische Systeme zur Bildung von Verbraucherprofilen oder der Erstellung von Verhaltensprognosen eingesetzt werden. Als allgemeines Risiko gilt gegenwärtig, dass algorithmische Systeme gesellschaftliche Ungleichheit festigen und ungerechtfertigte Diskriminierungen fortschreiben können, wenn beispielsweise in den (Trainings-)Daten bereits Benachteiligungen enthalten sind. Hierdurch können insbesondere die Handlungsfreiheit, die Chancengleichheit und die Selbstbestimmung von Verbraucherinnen und Verbrauchern gefährdet werden.

   a) Auf welches Ziel hin, mit welchem Aufwand (gemessen in Vollzeitäquivalenten) und mit welchen bisherigen Ergebnissen wird die gegenwärtige Rechtslage „laufend“ überprüft, wie in der Maßnahme „Algo-

rithmenbasierte Entscheidungen überprüfbar machen“ im Rahmen der Umsetzungsstrategie „Digitalisierung gestalten“ ausgewiesen?

Entsprechend der Umsetzungsstrategie „Digitalisierung gestalten“ wird die gegenwärtige Rechtslage mit dem Ziel fortlaufend daraufhin überprüft, ob die bestehenden Regelungen ausreichend sind, um unzulässige Diskriminierungen beim Einsatz algorithmischer Systeme zu verhindern. Dieses Thema wird neben vielen weiteren digitalpolitischer Aspekten von der Bundesregierung bearbeitet. Der zeitliche Aufwand lässt sich daher nicht beziffern.

b) Welche Handlungsoptionen wurden, wie in der Maßnahme „Algorithmenbasierte Entscheidungen überprüfbar machen“ im Rahmen der Umsetzungsstrategie „Digitalisierung gestalten“ angekündigt, bislang erarbeitet?

Die Datenethikkommission hat am 23. Oktober 2019 ihre Empfehlungen an die Bundesregierung übergeben. Darin wurden ethische Maßstäbe entwickelt sowie konkrete Regulierungsoptionen in den Bereichen Umgang mit Daten, Algorithmenbasierte Entscheidungen und Künstliche Intelligenz vorgeschlagen. Die Bundesregierung wertet diese derzeit aus und prüft, ob und welche konkreten Maßnahmen auf nationaler und europäischer Ebene unter Einbeziehung internationaler Diskussionen unter anderem in Bezug auf die Regulierung von algorithmischen Systemen erforderlich sind.

Auf europäischer Ebene wird die Bundesregierung im Rahmen des Konsultationsprozesses zum Weißbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ der Europäischen Kommission eine Stellungnahme erarbeiten. Dabei wird auch geprüft, ob bzw. wie die Ergebnisse der Datenethikkommission berücksichtigt werden können.

c) In welchem rechtlichen, organisatorischen oder finanziellen Zusammenhang steht die Maßnahme „Algorithmenbasierte Entscheidungen überprüfbar machen“ im Rahmen der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ mit der Datenethikkommission der Bundesregierung?

Bei der Datenethikkommission handelt es sich ebenfalls um eine Maßnahme im Rahmen der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“. Bei der Maßnahme „Algorithmenbasierte Entscheidungen überprüfbar machen“ werden auch die Empfehlungen der Datenethikkommission in die Prüfung miteinbezogen. Ein rechtlicher, organisatorischer oder finanzieller Zusammenhang besteht nicht.

d) Bis wann sollen die Empfehlungen der Datenethikkommission ausgewertet und entschieden werden, „ob und welche konkreten Maßnahmen auf nationaler und europäischer Ebene unter Einbeziehung internationaler Diskussionen unter anderem in Bezug auf die Regulierung von algorithmischen Systemen erforderlich sind“, wie in der Antwort der Bundesregierung auf Bundestagsdrucksache 19/14838 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14307, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten‘ – Algorithmenbasierte Entscheidungen überprüfbar machen“, angekündigt?

Die Empfehlungen der Datenethikkommission werden derzeit von der Bundesregierung ausgewertet und geprüft. Die Prüfung dauert an und wird auch neue Entwicklungen, etwa auf europäischer Ebene, einbeziehen.

10. Wie viele der 34 bislang existierenden Digital-Kompass-Standorte (Antwort der Bundesregierung auf Bundestagsdrucksache 19/14994, auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14448, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten' – Digitale Kompetenzen von Verbraucherinnen und Verbrauchern fördern") wurden durch das Projekt „Digital-Kompass plus" innerhalb der Maßnahme „Digitale Kompetenzen von Verbraucherinnen und Verbrauchern fördern" der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten" neu erschlossen, und wie viele bereits bestehende Standorte wurden lediglich ausgebaut?

Der Digital-Kompass ist ein Projekt der Bundesarbeitsgemeinschaft der Senioren-Organisationen e. V. und Deutschland sicher im Netz e. V. Dementsprechend richten sich die Angebote des Projektes hauptsächlich an ältere Verbraucherinnen und Verbraucher mit dem Ziel, ihre digitalen Kompetenzen zu stärken.

Zentral hierfür sind Digital-Kompass-Standorte, die als Anlaufstellen der ehrenamtlichen Multiplikatorinnen und Multiplikatoren und interessierten Verbraucherinnen und Verbrauchern dienen. Im Projekt wurden mittlerweile insgesamt 44 Standorte eröffnet und seither fortlaufend durch das Projektteam betreut.

Weitere 20 Standorte sind derzeitig in der Planung. Neu bei allen Standorten ist die Weiterqualifizierung der Internetlotsinnen und Internetlotsen durch Digital-Kompass-Materialien und digitale Formate wie Digitale Stammtische.

a) Um welche bestehenden Standorte, z. B. Volkshochschulen, handelt es sich dabei (bitte jeweils nach Städten oder Gemeinden auflisten)?

Die Liste der bestehenden Standorte des Projektes ist unter der Website www.digital-kompass.de/standorte öffentlich abrufbar.

b) Welche Materialien, z. B. Anleitungen, und Dienstleistungen, z. B. digitale Sprechstunden, werden nach Kenntnis der Bundesregierung von den Standorten jeweils in welchen Quantitäten erbracht (bitte jeweils nach Städten oder Gemeinden auflisten)?

Sämtliche Materialien werden für alle Standorte in gleichem Umfang und in gleicher Qualität angeboten und nach einer entsprechenden Rückmeldung bedarfsgerecht ausgeliefert. Jeder Standort kann an den „Digitalen Stammtischen" des Projektes teilnehmen.

c) Wie viele Verbraucherinnen und wie viele Verbraucher wurden durch die Materialausgabe und durch die Erbringung von Dienstleistungen von allen Standorten nach Kenntnis der Bundesregierung insgesamt erreicht (bitte nach den im Projekt gewählten soziodemographischen Merkmalen Alter und Migrationsstatus aufgliedern)?

Das Projekt erreicht über die Standorte vorrangig Multiplikatorinnen und Multiplikatoren, die ihrerseits ihre Kenntnisse an die Verbraucherinnen und Verbraucher weitergeben. Nach Aussage des Zuwendungsempfängers hat das Projekt schätzungsweise ca. 20.000 Verbraucherinnen und Verbraucher erreicht. Soziodemografische Daten werden nicht erfasst.

d) Aus welchen Gründen wurden zur Ausgestaltung des Beratungsangebotes der Standorte die Verbraucher und Verbraucherinnen nach den soziodemographischen Merkmalen Alter und Migrationsstatus diskriminiert und nicht z. B. nach den Merkmalen Geschlecht oder Einkommen?

Es wird auf Absatz 1 der Antwort zu Frage 10 und Satz 3 der Antwort zu Frage 10c verwiesen.

e) Welche empirischen Erkenntnisse liegen der Bundesregierung vor, die einen überproportionalen Mangel an „grundlegenden digitalen Kompetenzen“, wie sie laut Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ im Rahmen der Maßnahme „Digitale Kompetenzen von Verbraucherinnen und Verbrauchern fördern“ vermittelt werden sollen (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 20), bei Personen mit Migrationshintergrund belegen?

Der Bundesregierung liegen keine empirischen Erkenntnisse vor, die für einen überproportionalen Mangel an „grundlegenden digitalen Kompetenzen“ bei der genannten Personengruppe sprechen.

f) Wie viele ehrenamtliche Akteure unterstützen derzeit die Digital-Kompass-Standorte nach Kenntnis der Bundesregierung (bitte nach Geschlecht, Migrationsstatus und Standorten aufschlüsseln)?

Insgesamt ca. 300 bis 350 ehrenamtliche Seniorinnen und Senioren unterstützen die derzeit 44 Digital-Kompass-Standorte. Weitere soziodemografische Daten werden nicht erfasst.

g) Wie viele ehrenamtliche Akteure haben nach Kenntnis der Bundesregierung ihr Engagement bereits wieder eingestellt, und aus welchen Gründen?

Es ist nicht bekannt, ob und wie viele Ehrenamtliche während der Projektlaufzeit ihr Engagement eingestellt haben.

11. Welche konkreten Ergebnisse haben die bisherigen drei Veranstaltungen (Antwort der Bundesregierung auf Bundestagsdrucksache 19/15102 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14278, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten‘ – Allgemeine Compliance-Standards für Telemedien entwickeln“) des Formats „Zukunftsdialog Soziale Netzwerke“ zu den in der Maßnahme „Allgemeine Compliance-Standards für Telemedien entwickeln“ der Umsetzungsstrategie „Digitalisierung gestalten“ definierten Projektzielen der „Stärkung der Rechte der Nutzerinnen und Nutzer bei sozialen Netzwerken vor unberechtigten Löschungen und Sperrungen“ sowie der „Stärkung der Datenportabilität und Interoperabilität bei Sozialen Netzwerken und Messenger-Diensten“ beigetragen?

Der vom Bundesministerium der Justiz und für Verbraucherschutz durchgeführte „Zukunftsdialog Soziale Netzwerke“ hat sich mit der Rechtsstellung der Nutzerinnen und Nutzer sozialer Netzwerke gegenüber den Plattformanbietern und mit Fragen des Bedarfs und gegebenenfalls Optionen zur Stärkung der Nutzerrechte befasst. Die Erörterungen sind eingeflossen in den vom Bundesministerium der Justiz und für Verbraucherschutz im Januar 2020 vorgelegten Referentenentwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes. Der Entwurf sieht zur Stärkung der Nutzerrechte unter anderem ein

sog. Gegenvorstellungsverfahren vor, mit dem der Beschwerdeführer bzw. der Inhalteverfasser eine nochmalige Überprüfung der Entscheidung des Anbieters eines sozialen Netzwerks, einen Inhalt zu löschen oder nicht zu löschen, herbeiführen kann.

Die Stärkung der Datenportabilität und Interoperabilität bei sozialen Netzwerken und Messenger-Diensten ist nicht Gegenstand der Erörterungen im Zukunftsdialog Soziale Netzwerke.

a) Aus welchem Grund widmeten sich, wie aus der Antwort der Bundesregierung auf Bundestagsdrucksache 19/15102 auf Kleine Anfrage der AfD-Fraktion auf Bundestagsdrucksache 19/14278, „Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung ‚Digitalisierung gestalten' – Allgemeine Compliance-Standards für Telemedien entwickeln", hervorgeht, die bisherigen drei Veranstaltungen des Formats „Zukunftsdialog Soziale Netzwerke" ausschließlich der Bekämpfung von Hassrede, obwohl die übergeordnete Maßnahme auf die „Entwicklung allgemeiner Compliance-Standards für Telemedien" abzielt und deren Projektziele eindeutig als „Stärkung der Rechte der Nutzerinnen und Nutzer bei sozialen Netzwerken vor unberechtigten Löschungen und Sperrungen" sowie als „Stärkung der Datenportabilität und Interoperabilität bei Sozialen Netzwerken und Messenger-Diensten" definiert sind?

Um auf die Ziele des Abschnitts „Allgemeine Compliance-Standards für Telemedien entwickeln" der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten" hinzuarbeiten, werden mehrere Maßnahmen genutzt. Eine dieser Maßnahmen bildet der Zukunftsdialog Soziale Netzwerke.

b) Welche technischen und rechtlichen Detailfragen werden derzeit im Rahmen des im März 2019 begonnenen schriftlichen Konsultationsmechanismus des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) (ebenda) besprochen?

c) Zu welchen Ergebnissen hat der schriftliche Konsultationsmechanismus geführt?

d) Bis wann soll die Auswertung der Ergebnisse des schriftlichen Konsultationsmechanismus durch das BMJV abgeschlossen sein?

e) Bis wann soll die „Entwicklung von Konzept-/Eckpunktepapieren zu Handlungsoptionen", wie sie in der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten" seit November 2018 (https://www.bundesfinanzministerium.de/Content/DE/Downloads/Digitalisierung/2018-11-15-Digitalisierung-gestalten.pdf?__blob=publicationFile&v=2, S. 55) angekündigt wird, im Rahmen der Maßnahme „Allgemeine Compliance-Standards für Telemedien entwickeln" abgeschlossen sein?

Die Fragen 11b bis 11e werden gemeinsam beantwortet.

Der europäische Kodex für die elektronische Kommunikation (Richtlinie (EU) 2018/1972) stellt an eine Interoperabilitätsverpflichtung von rufnummernunabhängigen interpersonellen Kommunikationsdiensten (z. B. Skype, WhatsApp, Telegram, Facebook Messenger) hohe Anforderungen. Die Bundesregierung wird bei der anstehenden Umsetzung in nationales Recht im Rahmen des Umsetzungsspielraumes prüfen, unter welchen Bedingungen im Sinne des Koalitionsvertrages Handlungsmöglichkeiten bestehen. Die Bundesnetzagentur führt unabhängig davon eine Verbraucherbefragung zu der Nutzung interpersoneller Kommunikationsdienste durch, um mehr empirische Daten zu erlangen.

Zu verbraucherpolitischen Fragen der Interoperabilität und Datenportabilität speziell bei sozialen Netzwerken hat das Bundesministerium der Justiz und für

Verbraucherschutz in der ersten Jahreshälfte 2019 eine Konsultation ausgewählter Interessenvertreter durchgeführt. Gegenstand der Konsultation waren die Vor- und Nachteile der Interoperabilität bei sozialen Netzwerken aus Nutzer-, Anbieter- und Wettbewerbssicht sowie alle damit im Zusammenhang stehenden rechtlichen und technischen Fragen und Probleme. Hinsichtlich Datenportabilität wurden die Konsultationsteilnehmer nach Möglichkeiten zur Behebung von Anwendungsdefiziten der entsprechenden Datenschutz-Grundverordnungsregelung in der konkreten Praxis sozialer Netzwerke gefragt. Im Ergebnis dieser Konsultation überwogen insgesamt hinsichtlich Interoperabilitätsvorgaben die kritischen Stimmen (rechtliche und technische Risiken, Komplexität), hinsichtlich der Datenportabilität wurden die Probleme vorwiegend bei fehlenden einheitlichen Formaten und Standards am Markt gesehen. Die Bundesregierung plant gegenwärtig mit Blick auf sich bereits abzeichnende Entwicklungen auf EU-Ebene kein gesetzgeberisches Handeln. Die EU-Kommission hat am 19. Februar 2020 in ihrer Mitteilung zu einer europäischen Datenstrategie unter anderem angekündigt, im Zusammenhang mit dem Ziel der Stärkung der Rechte der Betroffenen auch Möglichkeiten der Weiterentwicklung und Stärkung des Portabilitätsrechts nach Artikel 20 Datenschutz-Grundverordnung prüfen zu wollen, einschließlich möglicher Vorgaben zu Schnittstellenstandards oder Datenformaten. Entsprechende Regelungen könnten gemäß den Ankündigungen der EU-Kommission gegebenenfalls in den für das Jahr 2021 anvisierten Vorschlag für einen Rechtsakt über Daten („Data Act“) aufgenommen werden.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333