

Antwort der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Christian Lindner, Stephan Thomae,
Michael Theurer, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/2278 –**

Anwendbarkeit der Datenschutz-Grundverordnung

Vorbemerkung der Fragesteller

Ab 25. Mai 2018 wird die 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 (DSGVO)) anwendbar sein. Damit beginnt ein neues Kapitel in der Geschichte des Datenschutzes. Ziel der DSGVO ist es, einheitliche Datenschutzregelungen in der EU zu schaffen, was den Bürgerinnen und Bürgern aber auch grenzüberschreitend tätigen Unternehmen zugutekommt. Ferner ist das europäische Datenschutzrecht nunmehr auch eindeutig auf Anbieter von Waren und Dienstleistern ohne Niederlassung in der EU anwendbar. Schließlich sieht die DSGVO im Vergleich zur bisherigen Rechtslage drastisch erhöhte Sanktionen vor (bis zu 20 Mio. Euro oder 4 Prozent des weltweiten Jahresumsatzes).

Auch angesichts dieser hohen Bußgelder ist die Unsicherheit in der deutschen Wirtschaft groß. So sahen sich noch im April 2018 lediglich 13 Prozent aller Unternehmen nach einer Umfrage im Auftrag des Verbands der Internetwirtschaft eco auf die DSGVO rechtlich gut vorbereitet (<https://www.eco.de/presse/eco-verband-dsgvo-haelt-deutsche-wirtschaft-in-atem/>). Dies wirft die Frage auf, welche Maßnahmen die Bundesregierung ergriffen hat, um die deutsche Wirtschaft auf die DSGVO vorzubereiten, zumal die Unruhe in der deutschen Wirtschaft nicht zur Akzeptanz der Bedeutung des Datenschutzes für die Bürgerinnen und Bürger sowie eine demokratische Gesellschaft beitragen dürfte. In einigen Punkten ist der deutsche Gesetzgeber zudem über die Verpflichtungen der DSGVO hinausgegangen. Dies betrifft insbesondere die Verpflichtung zur Stellung eines Datenschutzbeauftragten, sobald zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG) n. F.). Da praktisch jeder Arbeitnehmer heute mit der automatisierten Verarbeitung von personenbezogenen Daten betraut ist (z. B. Kundendaten oder Beschäftigtendaten), bedeutet dies faktisch, dass nahezu jeder Betrieb mit zehn Arbeitnehmern einen Datenschutzbeauftragten stellen muss. Die Anzahl der Beschäftigten hat jedoch nichts mit dem Risiko der Datenverarbeitung zu tun und ist daher schon früher als sachfremd kritisiert worden (vgl. zur Kritik bereits Simitis in Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 4f Rn. 16).

Eine weitere Quelle der Unruhe in der deutschen Wirtschaft ist die Rechtsunsicherheit. Eine Ursache hierfür ist, dass der deutsche Gesetzgeber viele praxisrelevante Regelungen z. B. im Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) oder Kunsturhebergesetz (KUG), welches die Veröffentlichung von Bildern regelt, vor dem 25. Mai 2018 nicht an die DSGVO angepasst haben wird und die Auswirkungen auf andere Bereiche (wie z. B. die Verwendung von Cookies, welche für das Webtracking und personalisierte Werbung im Internet erforderlich sind) unklar sind.

Viele Fragen werden erst in mehreren Jahren durch den Europäischen Gerichtshof geklärt werden können. Bis dahin werden die Leitlinien des Europäischen Datenschutzausschusses von großer Bedeutung sein. Dort werden die deutschen Aufsichtsbehörden von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vertreten. Diese kann die für die nächsten Jahre in der Praxis maßgeblichen Leitlinien mitbestimmen; Voraussetzung sind hierfür aber ausreichende Ressourcen, da die Entwürfe der Leitlinien von den nationalen Aufsichtsbehörden erarbeitet werden. Ein weiteres Mittel zur Reduzierung von Rechtsunsicherheit können die neuen Instrumente der Selbstregulierung sein, welche die DSGVO einführt. Voraussetzung hierfür ist, dass diese von den Unternehmen akzeptiert werden und dass es – im Falle der Zertifizierung – ausreichend unabhängige Zertifizierungsstellen gibt.

Große Unsicherheit besteht zudem im Hinblick auf die Regelungen, welche ab dem 25. Mai 2018 auf die Veröffentlichung von Bildern von Personen Anwendung finden. Bisher wurde die Zulässigkeit der Veröffentlichung in der Praxis nach den §§ 22 ff. KUG beurteilt. Es stellt sich nun ab dem 25. Mai 2018 die Frage, ob diese Regelungen noch Bestand haben werden, soweit sie sich mit dem Anwendungsbereich der DSGVO überschneiden, und welche Regelungen stattdessen gelten werden.

I. Vorbereitung der Wirtschaft

1. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Wirtschaft bei der Umstellung auf die DSGVO zu unterstützen?

Die Bundesregierung steht seit Monaten mit Unternehmen, Wirtschaftsverbänden und Kammern zu Fragen der Umsetzung der Verordnung (EU) 2016/679 in engem Austausch. Seit Oktober 2017 führt das Bundesministerium für Wirtschaft und Energie gemeinsam mit dem Bundesministerium des Innern, für Bau und Heimat kontinuierliche Round-Table-Gespräche zur Umsetzung der Verordnung (EU) 2016/679 mit Vertretern der Wirtschaft und der Datenschutzaufsichtsbehörden.

Zudem hat das Bundesministerium für Wirtschaft und Energie im Rahmen einer gemeinsam mit dem Deutschen Industrie- und Handelskammertag organisierten „Road Show“ zur Verordnung (EU) 2016/679 von Februar bis Mai 2018 deutschlandweit über 30 Informationsveranstaltungen zur Verordnung (EU) 2016/679 vor Ort begleitet.

2. Welche Mittel wurden hierfür aufgewandt?

Eine gesonderte Erfassung der von Personal- und Sachmittel ist nicht erfolgt. Der Aufwand kann daher nicht beziffert werden.

3. Ist die Bundesregierung der Auffassung, dass die deutsche Wirtschaft – vor allem klein- und mittelständische Unternehmen – gut auf die Anwendbarkeit der DSGVO vorbereitet sind?

Wenn nein, worauf führt die Bundesregierung dies zurück?

Die Bundesregierung hat keine eigenen Umfragen zu dem Thema durchgeführt, wie sich die deutsche Wirtschaft und insbesondere die klein- und mittelständischen Unternehmen auf die Anwendbarkeit der Verordnung (EU) 2016/679 vorbereitet haben. Sie hat aber durch die in der Antwort zu Frage 1 genannten Maßnahmen rechtzeitig die Initiative ergriffen, um die Wirtschaft bei der Rechtsanpassung zu unterstützen und über den Rechtsakt zu informieren.

4. Welche weiteren Maßnahmen plant die Bundesregierung hierzu?

Die Bundesregierung wird den Austausch mit der Wirtschaft und den Datenschutzaufsichtsbehörden fortführen, um hieraus Erkenntnisse zu gewinnen, wie die praktische Umsetzung in der Wirtschaft erfolgt und welche Probleme bei der Umsetzung in der Praxis bestehen.

Es ist geplant, die FAQs zur Verordnung (EU) 2016/679 des Bundesministeriums des Innern, für Bau und Heimat (abrufbar unter <https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/04/faqs-datenschutz-grundverordnung.html>), die bereits zahlreiche Antworten auf die wichtigsten Fragen zu den Neuerungen der Verordnung (EU) 2016/679 geben und den Einstieg in die Rechtsmaterie erleichtern sollen, unter Berücksichtigung der gewonnenen Erkenntnisse fortzuschreiben.

5. Welche Maßnahmen hat die Bundesregierung unternommen, um Unternehmen für die Bedeutung des Datenschutzes zu sensibilisieren?

Auf die Antwort zu Frage 1 wird verwiesen.

Ergänzend wird darauf hingewiesen, dass die Sensibilisierung der Unternehmen für die Bedeutung des Datenschutzes eine gemeinsame Aufgabe der Bundesregierung, der Datenschutzaufsichtsbehörden von Bund und Ländern und der Verbände sowie der Kammern ist.

II. Beschäftigtendatenschutz

6. Plant die Bundesregierung zusätzliche Regelungen zum Arbeitnehmerschutz?

Wenn ja, mit welchem Inhalt und welchem Zeitplan?

Die Bundesregierung wird die im Koalitionsvertrag zwischen CDU, CSU und SPD (vgl. Rn. 6002) vereinbarte Prüfung zur Schaffung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz vornehmen. Inhalte oder Zeitpläne hierzu stehen noch nicht fest.

7. Hat die Bundesregierung Kenntnis darüber, welche zusätzlichen Kosten der Wirtschaft dadurch entstehen, dass § 26 Absatz 2 Satz 3 BDSG n. F. – abweichend von der DSGVO – im Arbeitsverhältnis zwingend an der Schriftform der Einwilligung festhält?

Die Bundesregierung hat keine Kenntnisse, welche Kosten der Wirtschaft aufgrund der abweichenden Regelung zur Schriftform in § 26 Absatz 2 Satz 3 BDSG (2018) entstehen. Die Regelung in § 26 Absatz 2 Satz 3 BDSG 2018 führt die Rechtslage fort, die vor dem Wirksamwerden der Verordnung (EU) 2016/679 zur Einwilligung bei Arbeitsverhältnissen bestand.

III. Datenschutzaufsichtsbehörden

8. Sind nach Ansicht der Bundesregierung die Datenschutzaufsichtsbehörden ausreichend personell und sachlich ausgestattet, um ihre Aufgaben zu erfüllen, insbesondere Verantwortliche und Auftragsdatenverarbeiter über ihre Pflichten nach der DSGVO zu sensibilisieren (Artikel 57 Absatz 1 Buchstabe d DSGVO) und ihre Befugnisse zur Beratung und Genehmigung auszuüben (Artikel 58 Absatz 2 DSGVO)?

Wenn nein, welche Maßnahmen erscheinen nach Ansicht der Bundesregierung hierfür erforderlich?

9. Ist nach Ansicht der Bundesregierung die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ausreichend ausgestattet, um ihre Aufgaben als zentrale Anlaufstelle und gemeinsame Vertreterin im Europäischen Datenschutzausschuss nach §§ 17 ff. BDSG ausüben zu können?

Wenn nein, welche Maßnahmen plant die Bundesregierung zu ergreifen?

10. Ist die BfDI nach Ansicht der Bundesregierung ausreichend ausgestattet, um bei der Erarbeitung von Leitlinien und Empfehlungen des Europäischen Datenschutzausschusses (Artikel 70 Absatz 1 DSGVO) eine maßgebliche Rolle spielen zu können?

Die Fragen 8 bis 10 werden wegen des Sachzusammenhangs zusammen beantwortet.

Die Bundesregierung erachtet eine angemessene Ausstattung der BfDI sowie der Datenschutzaufsichtsbehörden der Länder für wichtig und notwendig, damit diese Behörden ihre gesetzlichen Aufgaben effizient und wirkungsvoll ausführen können.

In der Begründung zum Entwurf des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU) hatte die Bundesregierung deshalb z. B. die Forderung der BfDI, zehn Stellen für die Wahrnehmung der Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss und der zentralen Anlaufstelle zu erhalten, aufgenommen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sind gemäß den EU-rechtlichen Vorgaben unabhängige Behörden. Etwaigen Personalbedarf müssen sie selbständig bei dem für die Aufstellung des Haushaltsplanes zuständigen Finanzministerium anmelden. Für die Ausstattung der Datenschutzaufsichtsbehörden der Länder sind die Länder (und damit letztlich die Landesparlamente) zuständig.

Die BfDI bringt als unabhängige oberste Bundesbehörde ihre Personal- und Sachmittelansätze in das Verfahren zur Aufstellung des Bundeshaushaltsplanes (Einzelplan 21) selbständig ein. Eine entsprechende Ausstattung der unabhängigen

Datenschutzaufsichtsbehörden mit den erforderlichen Personal- und Sachmitteln muss der Deutsche Bundestag als Haushaltsgesetzgeber bewilligen.

Im Haushalt 2017 hat die BfDI in einem ersten Schritt zur Umsetzung der Datenschutz-Grundverordnung 32 neue Planstellen/Stellen erhalten. Für die Haushaltsjahre 2018 und 2019 wurden weitere Planstellen/Stellen für die Umsetzung der Verordnung (EU) 2016/679 angemeldet. Darüber wird zurzeit mit der BfDI im Rahmen der Aufstellung der Bundeshaushalte 2018 und 2019 verhandelt.

11. Ist die Bundesregierung der Ansicht, dass es aufgrund der DSGVO für klein- und mittelständische Unternehmen zu höheren Bußgeldern als bisher in der Praxis kommen wird?

Die Bundesregierung ist nicht der Ansicht, dass es aufgrund der Verordnung (EU) 2016/679 für klein- und mittelständische Unternehmen zu höheren Bußgeldern als bisher in der Praxis kommen wird. Die unabhängigen Datenschutzaufsichtsbehörden in den Ländern haben eine langjährig geübte Praxis bei der Verhängung von verhältnismäßigen Sanktionen. Die Bundesregierung hat keine Anhaltspunkte dafür, dass die Datenschutzaufsichtsbehörden von dieser Praxis einer verhältnismäßigen Sanktionierung abweichen werden, die auch durch das EU-Recht ausdrücklich vorgegeben ist.

Bundesminister Horst Seehofer hat mit Schreiben vom 30. Mai 2018 an die Vorsitzende der Datenschutzkonferenz (DSK) auf Fortsetzung der Verhängung von Bußgeldern mit Augenmaß geworben.

12. Wie kann aus Sicht der Bundesregierung bei der Bemessung von Bußgeldern und anderen Sanktionen der besonderen Situation von kleinen und mittleren Unternehmen (KMUs) Rechnung getragen werden, deren Kerngeschäft nicht die Verarbeitung personenbezogener Daten ist?

Bei der Verhängung von Geldbußen ist das im europäische Recht verankerte Gesetzlichkeitsprinzip zu beachten (Artikel 7 Europäische Menschenrechtskonvention EMRK und Artikel 49 Charta der Grundrechte der Europäischen Union), welches ein Verbot eines strafbegründenden und strafschärfenden Gewohnheitsrechts, das Bestimmtheitsgebot, das Rückwirkungs- und das Analogieverbot enthält. Darüber hinaus ist bei einer Sanktionierung der Grundsatz der Verhältnismäßigkeit zu berücksichtigen, der in Artikel 83 Absatz 1 der Verordnung (EU) 2016/679 auch ausdrücklich angesprochen wird. Dieser Grundsatz wirkt begrenzend hinsichtlich der Frage, ob eine Geldbuße erlassen wird und ebenfalls hinsichtlich der Höhe der Geldbuße. Artikel 83 Absatz 2 der Verordnung (EU) 2016/679 führt darüber hinaus einen Katalog von Zumessungskriterien auf. Dieser ist in jedem Einzelfall gebührend von den Datenschutzaufsichtsbehörden bei der Verhängung einer Geldbuße zu berücksichtigen, sodass den besonderen Situationen von kleinen und mittleren Unternehmen (KMUs) Rechnung getragen werden kann.

13. Wie hoch schätzt die Bundesregierung die zusätzliche Belastung für die deutsche Wirtschaft durch Bußgelder pro Jahr?

Auf die Antworten zu den Fragen 11 und 12 wird verwiesen.

Der Bundesregierung liegen darüber hinaus keine Erkenntnisse vor, wie die Datenschutzaufsichtsbehörden künftig Bußgelder verhängen werden.

IV. Selbstregulierung

14. Hält die Bundesregierung Verhaltensregeln nach Artikel 40 DSGVO für ein geeignetes Instrument, um die Unsicherheit in der täglichen Rechtsanwendung in Unternehmen zu verringern?

Die Bundesregierung hält Verhaltensregeln nach Artikel 40 der Verordnung (EU) 2016/679 für ein geeignetes Instrument, um die Unsicherheit in der täglichen Rechtsanwendung in Unternehmen zu verringern.

15. Hat die Bundesregierung Erkenntnisse darüber, ob bereits Verhaltensregelungen nach Artikel 40 DSGVO genehmigt worden sind oder in Vorbereitung sind?

Wenn ja, welche?

Die Bundesregierung hat durch die gemeinsamen Informationsveranstaltungen des BMI und des BMWi zur Umsetzung der Verordnung (EU) 2016/679 (vgl. Antwort zu Frage 1) sowie durch eine durch das BMWi im Februar 2018 an ausgewählte Wirtschaftsverbände gerichtete Best-Practice-Abfrage zum Umsetzungsstand der Verordnung (EU) 2016/679 in den Unternehmen von mehreren Verbänden Rückmeldungen zu der Frage erhalten, ob Codes of Conduct geplant bzw. erarbeitet werden. Nach den der Bundesregierung vorliegenden Erkenntnissen sind mehrere Verbände gegenwärtig in verschiedenen Stadien mit der Vorbereitung von branchenspezifischen Codes of Conduct befasst. Teilweise erfolgen diese Arbeiten auf europäischer Ebene.

16. Sind bereits Zertifizierungsstellen nach Artikel 43 DSGVO akkreditiert worden?

Wie viele Zertifizierungsstellen wird es mit Anwendbarkeit der DSGVO am 25. Mai 2018 in der Bundesrepublik Deutschland geben?

Hält die Bundesregierung diese Zahl für ausreichend?

Wenn nein, welche Maßnahmen wird die Bundesregierung ergreifen, um ihre Zahl zu erhöhen?

Es war bislang nicht möglich (Stand: 6. Juni 2018) Zertifizierungsstellen nach Artikel 43 in Verbindung mit Artikel 42 Absatz 5 der Verordnung (EU) 2016/679 und Überwachungsstellen nach Artikel 43 in Verbindung mit Artikel 41 Absatz 2 der Verordnung (EU) 2016/679 im Bereich des Datenschutzes zu akkreditieren und von den zuständigen Bundes- oder Landesdatenschutzbehörden zuzulassen, weil der Europäische Datenschutzausschuss gemäß Artikel 68 der Verordnung (EU) 2016/679 zunächst ein Verfahren zur Meldung der Akkreditierungskriterien gemäß Artikel 43 Absatz 6 Satz 2 der Verordnung (EU) 2016/679 bereitstellen muss. Außerdem konnte sich der Europäische Datenschutzausschuss erst ab dem 25. Mai 2018 konstituieren. Ein entsprechendes Meldeverfahren steht derzeit noch nicht zur Verfügung.

Zertifizierungen können durch die Datenschutzaufsichtsbehörden (Artikel 42 Absatz 5 der Verordnung (EU) 2016/679) oder Zertifizierungsstellen nach Artikel 43 der Verordnung (EU) 2016/679 erfolgen. Mit Wirksamwerden der Verordnung (EU) 2016/679 am 25. Mai 2018 können somit 22 Stellen Zertifizierungen vornehmen. Die Bundesregierung hat keine Anhaltspunkte dafür, dass diese Anzahl von möglichen Stellen, die Zertifizierungen vornehmen können, zu Beginn des Wirksamwerdens der Datenschutz-Grundverordnung nicht ausreichend ist.

17. Sind Verbände und Unternehmen nach Ansicht der Bundesregierung ausreichend über die Möglichkeiten der Verwendung genehmigter Verhaltensregeln und das Instrument der Zertifizierung informiert?

Wenn nein, welche Maßnahmen plant die Bundesregierung hierzu?

18. Welche Maßnahmen hat die Bundesregierung bisher ergriffen?

Die Fragen 17 und 18 werden wegen des Sachzusammenhangs zusammen beantwortet.

Nach Auffassung der Bundesregierung sind die Verbände ausreichend informiert. In den gemeinsamen Informationsveranstaltungen des BMI und des BMWi zur Umsetzung der Verordnung (EU) 2016/679 (vgl. Antwort zu Frage 1) wurden mehrfach die Instrumente und die Möglichkeiten der Selbstregulierung (z. B. Code of Conducts i. S. v. Artikel 40 der Verordnung (EU) 2016/679) erörtert.

Die Bundesregierung will Unternehmen dabei unterstützen, die neuen Regeln der Verordnung (EU) 2016/679 umzusetzen und diesen Rechtsrahmen mit innovativen Geschäftsmodellen zu füllen. Dazu gehört, dass Cloud- Dienste weiterhin einfach und rechtskonform nutzbar sein müssen, denn sie sind zentral für die Wirtschaft und ihre weitere Digitalisierung. Mit dem Projekt AUDITOR hat sich die Bundesregierung zum Ziel gesetzt, Anbietern wie Nutzern von Cloud- Diensten eine Datenschutzzertifizierung an die Hand zu geben, die europaweit anerkannt ist. Zertifizierte Produkte werden alle Vorteile einer Cloud bieten und dabei das Grundrecht auf Datenschutz sicherstellen. Das kann über die EU hinaus ein Wettbewerbsvorteil für unsere Unternehmen sein.

Für den für die Wirtschaft sehr wichtigen Bereich der Auftragsverarbeitung im Rahmen von Cloud Services sind darüber hinaus weitreichende Informationsaktivitäten durch das Kompetenznetzwerk Trusted Cloud erfolgt. Im Kompetenznetzwerk sind unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Energie wesentliche Verbände sowohl der Anbieter- (z. B. Bitkom, Bundesverband IT Mittelstand, eco Verband der Internetwirtschaft) als auch der Anwenderseite (z. B. VOICE Bundesverband der IT Anwender, ENX Association/VDA) sowie Unternehmen, speziell auch KMU organisiert.

Das Kompetenznetzwerk hat im Rahmen von Kooperationen mit weiteren Verbänden (z. B. Bundesverband Digitale Wirtschaft, Bundesverband mittelständische Wirtschaft, deutscher Industrie- und Handelskammertag, Zentralverband des Handwerks, Gesamtverband der Versicherungswirtschaft, Bundesverband IT Gesundheit, Gesellschaft für Informatik, Offensive Mittelstand, regionale Initiativen wie innozent OWL) auf über 50 Informationsveranstaltungen im Jahr 2018 über die Neuregelungen der der Verordnung (EU) 2016/679 und die möglichen Instrumente zur Dokumentation der Erfüllung der Anforderungen (Gütesiegel, genehmigte Verhaltensregeln gem. Artikel 40 der Verordnung (EU) 2016/679, Zertifikate gemäß Artikel 42 der Verordnung (EU) 2016/679) informiert.

Auf der Webpräsenz www.trusted-cloud.de wird speziell zum Thema der Verordnung (EU) 2016/679 auf einer dedizierten Seite Orientierungswissen insbesondere für kleine und mittelständische Anwenderunternehmen zur Verfügung gestellt. Zum Thema „DSGVO“ wurden auch Websessions, speziell auch zu den Themen genehmigter Verhaltensregeln als auch Zertifizierung vom Kompetenznetzwerk selbst und in Kooperation mit Unternehmen abgehalten.

In sämtlichen Presseaktivitäten des Kompetenznetzwerks ist über unterschiedliche Medien auf die Anforderungen der der Verordnung (EU) 2016/679 und auf den Stellenwert von Gütesiegeln, genehmigten Verhaltensregeln und Zertifikaten

hingewiesen worden. Das Kompetenznetzwerk steht als Anlaufstelle für Fragestellungen von Anbietern und Nutzern von Cloud-Diensten zur Verfügung.

Das Kompetenznetzwerk wird diese Informationsfunktion auch weiterhin auf unterschiedlichen Plattformen ausüben.

Im Rahmen der Trusted Cloud Initiative des Bundesministeriums für Wirtschaft und Energie wurde bereits im Rahmen des gleichnamigen Programms eine Zertifizierung (Trusted Cloud Datenschutzprofil-TCDP) entwickelt, welche es Cloud Anbietern ermöglicht, die Datenschutzkonformität auf Basis des BDSG a. F. nachzuweisen. Zertifizierungen auf dieser Basis sind von unabhängigen Prüfinstitutionen (TÜV, Dekra) durchgeführt worden.

Diese Zertifizierung wird aktuell im Rahmen des AUDITOR Projekts auf die aktuelle Rechtslage angepasst. Im Rahmen von AUDITOR, auch in Zusammenarbeit mit Aufsichtsbehörden, der nationalen Akkreditierungsstelle und des DIN, wird eine europaweit anwendbare Datenschutzzertifizierung entwickelt, welche den Anforderungen des Artikels 42 der Verordnung (EU) 2016/679 genügt. In dem Konsortium zur Erarbeitung des Zertifizierungsstandards sind sowohl Anbieter- als auch Anwenderunternehmen sowie Verbände als Partner integriert, so dass neben der Abdeckung aller relevanten fachlichen und juristischen Fragestellungen auch die Marktakzeptanz sichergestellt wird.

Die Zertifizierung wird durch DAkkS akkreditierte kompetente Prüfstellen durchgeführt werden. Die ersten Pilotzertifizierungen werden zum Jahreswechsel 2018/2019 erwartet.

Darüber hinaus wird vom Kompetenznetzwerk Trusted Cloud unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Energie ein Gütesiegel für Cloud Anwendungen herausgegeben. Dieses prüft unter Einbeziehung eines unabhängigen Auditors anhand eines mit Anwendern und Anbietern entwickelten Kriterienkatalogs die Einhaltung von Standards in den Bereichen Sicherheit, Vertragstransparenz, Funktionalität und auch Datenschutz. In der aktuellen Version 2.0 des Kriterienkatalogs sind die Anforderungen der Verordnung (EU) 2016/679 abgebildet. Dieses Gütesiegel sorgt für die aus Sicht der Wirtschaft dringend gebotene Transparenz.

Neben diesem Gütesiegel plant das Kompetenznetzwerk, im Rahmen von Kooperationen, die Erklärung der Konformität von Cloud Diensten an genehmigte Verhaltensregeln gemäß Artikel 40 der Verordnung (EU) 2016/679 als Prüfdienstleistung anzubieten. Speziell für mittelständische Anbieter werden diese genehmigten Verhaltensregeln ein wichtiges Instrument der Positionierung der angebotenen Dienste darstellen.

V. Anpassung des deutschen Rechts und Ausnutzung von Spielräumen durch den deutschen Gesetzgeber

19. Hat der deutsche Gesetzgeber der deutschen Wirtschaft über die DSGVO hinausgehende Verpflichtungen auferlegt?

Wenn ja, welche (bitte aufschlüsseln), und welche zusätzlichen Kosten werden diese nach Schätzung der Bundesregierung der deutschen Wirtschaft zusätzlich verursachen?

Ja. Ein Ziel der Bundesregierung bei der Anpassung des deutschen Datenschutzrechts an die Vorgaben der Datenschutz-Grundverordnung durch das DSAnpUG-EU war es, das nach dem BDSG a. F. bestehende Schutzniveau zu erhalten. Unter

Orientierung an dieser Rechtslage wurden folgende über die DSGVO hinausgehende Verpflichtungen vorgesehen:

- Schriftform der Einwilligung im Beschäftigtenverhältnis (§ 26 Absatz 2 Satz 3 BDSG – 2018): Da die Regelung die Rechtslage des BDSG a. F. fortführte (vgl. Antwort zu Frage 7), wurden keine weiteren Kostenschätzungen seitens der Bundesregierung vorgenommen.
- Bestellpflichten Datenschutzbeauftragte bei nichtöffentlichen Stellen (§ 38 Absatz 1 BDSG – 2018): Eine Kostenschätzung wurde seitens der Bundesregierung nicht vorgenommen, denn Pflichten zur Bestellung eines betrieblichen Datenschutzbeauftragten bestehen in Deutschland seit der Einführung des Bundesdatenschutzgesetzes im Jahr 1977 (BGBl. I vom 1. Februar 1977), so dass der Wirtschaft keine zusätzlichen Kosten durch neue Verpflichtungen entstehen.

20. Inwieweit fällt die Verarbeitung personenbezogener Daten im Rahmen von nicht öffentlichen Telekommunikationsnetzen (z. B. innerhalb von Unternehmen) unter die DSGVO?

Stehen die §§ 91 ff. TKG insoweit im Einklang mit der DSGVO oder sieht die Bundesregierung hier Anpassungsbedarf?

Warum ist eine Anpassung der §§ 91 ff. TKG bisher unterblieben, und wann plant die Bundesregierung diese?

Für die Verarbeitung personenbezogener Daten im Rahmen von nicht öffentlichen Telekommunikationsnetzen gilt uneingeschränkt die Verordnung (EU) 2016/679. Ein Gesetzentwurf zur Anpassung u. a. des TKG an die Verordnung (EU) 2016/679 ist in Vorbereitung.

21. Inwieweit stehen die §§ 11 ff. TMG mit der DSGVO im Einklang (bitte nach den einzelnen Regelungen aufschlüsseln)?

Sieht die Bundesregierung hier Anpassungsbedarf?

Wenn ja, warum ist eine Anpassung der §§ 11 ff. TMG bisher unterblieben, und wann plant die Bundesregierung diese?

Die Bundesregierung weist darauf hin, dass die DSK zur Nichtanwendbarkeit einiger Datenschutz-Regelungen des TMG hinsichtlich Reichweitenmessung und Tracking-Mechanismen und zu der Frage der Anwendung der Verordnung (EU) 2016/679 bei Telemedien und beim Einsatz von Tracking-Mechanismen einen Beschluss gefasst hat, der für die Rechtsanwendung durch die einzelnen unabhängigen Datenschutzaufsichtsbehörden von Bedeutung ist. Der Vollzug des Datenschutzrechts obliegt den unabhängigen Datenschutzbehörden. Die Bundesregierung hat darauf keinen Einfluss. Mit Blick auf die laufenden Verhandlungen für eine EU-Verordnung über den Schutz der Privatsphäre und der personenbezogenen Daten in der elektronischen Kommunikation (E-Privacy-V), hat die Bundesregierung die erforderliche Anpassung des TMG an die Verordnung (EU) 2016/679 zunächst zurückgestellt. Sie soll erfolgen, sobald die Verhandlungen zur E-Privacy-V abgeschlossen sind.

22. Ist nach Ansicht der Bundesregierung ab dem 25. Mai 2018 für die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits auf einem Endgerät gespeichert sind, insbesondere die Verwendung von Cookies, eine Einwilligung erforderlich, da nach Artikel 94 Absatz 2 DSGVO der Verweis auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zu lesen sind und Artikel 95 DSGVO nur die Bereitstellung öffentlich zugänglicher Informationsnetze betrifft?

Die Bundesregierung weist darauf hin, dass die Richtlinie 2002/58/EG im Gegensatz zur Richtlinie 95/46/EG nicht aufgehoben wurde. Daraus folgt, dass deren Bestimmungen unverändert Bestand haben. Dies gilt auch hinsichtlich Artikel 5 Absatz 3 der Richtlinie 2002/58/EG, der regelt, dass die Speicherung von und der Zugriff auf Informationen auf Endeinrichtungen nur gestattet ist, wenn der betreffende Nutzer auf der Grundlage von klaren und umfassenden Informationen nach dem Datenschutzrecht, u. a. über die Zwecke der Verarbeitung seine Einwilligung gegeben hat; dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

23. Sind nach Ansicht der Bundesregierung deutsche Datenschutzaufsichtsbehörden befugt, nationale Rechtsvorschriften, die nicht im Einklang mit der DSGVO stehen, nicht anzuwenden?

Bei der Kollision von nationalem Recht und Unionsrecht gilt grundsätzlich der Anwendungsvorrang des Unionsrechts.

24. Beobachtet die Bundesregierung die Anpassung des Datenschutzrechts in anderen Mitgliedstaaten an die DSGVO sowie die Nutzung der darin enthaltenen Spielräume durch die Gesetzgeber anderer Mitgliedstaaten?

Wenn ja, wie bewertet sie die dortige Anpassung und Nutzung von Spielräumen?

Gibt es nach Ansicht der Bundesregierung Regelungen, welche gegen die DSGVO verstoßen (z. B. in Österreich)?

Wenn ja, plant die Bundesregierung ein Vertragsverletzungsverfahren zum Schutze der deutschen Bürgerinnen und Bürger und zur Gewährleistung gleicher Wettbewerbsbedingungen für deutsche Unternehmen?

Die Bundesregierung verfolgt Anpassungen des nationalen Datenschutzrechts in anderen Mitgliedstaaten an die Verordnung (EU) 2016/679.

Die Europäische Kommission hat hierzu eine Expertengruppe eingesetzt, die sich regelmäßig auch unter Beteiligung von Deutschland trifft. Die EU-Mitgliedstaaten tragen zum Stand der Anpassungsarbeiten des nationalen Datenschutzrechts in dieser Expertengruppe allerdings nur abstrakt vor. Bewertungen einzelner Regelungen sind daher nicht möglich, zumal die entsprechenden Gesetzgebungsverfahren in den Mitgliedstaaten hierzu derzeit nicht abgeschlossen sind (wie z. B. in Österreich). Die Bundesregierung sieht derzeit keinen Anlass für eine Staatenklage (Artikel 259 AEUV).

25. Welche Anpassungen des deutschen allgemeinen und bereichsspezifischen Datenschutzrechts sind nach Ansicht der Bundesregierung aufgrund der jüngsten Berichtigungen der DSGVO (Amtsblatt der Europäischen Union L 119 vom 4. Mai 2018) erforderlich?

Falls diese erforderlich sind, wann plant die Bundesregierung sie umzusetzen?

Es sind keine Anpassungen erforderlich, da die jüngsten Berichtigungen nur reaktioneller Art waren.

26. Wie wird die Bundesregierung den gemäß Artikel 97 DSGVO zum 25. Mai 2020 (nach zwei Jahren) und danach alle vier Jahre von der Kommission zu erstellenden Bericht über die Bewertung und Überprüfung der Verordnung begleiten?

Mit welchem Prozess plant die Bundesregierung den Deutschen Bundestag in die Erstellung und Bewertung der Kommissions-Berichte einzubeziehen?

Die Bundesregierung wird die im Koalitionsvertrag (vgl. Rn. 6078) genannten Vorgaben zur Evaluierung der Verordnung (EU) 2016/679 aufgreifen. Demnach wird die Bundesregierung den Prozess zu Artikel 97 der Verordnung (EU) 2016/679 intensiv begleiten und dabei alle Regelungen auf ihre Zukunftsfähigkeit und Effektivität überprüfen. Der genaue Prozess hierzu steht noch nicht fest.

27. Ist nach Ansicht der Bundesregierung der Deutsche Bundestag eine der „anderen einschlägigen Stellen oder Quellen“, deren Standpunkte oder Feststellungen gemäß Artikel 97 Absatz 4 DSGVO von der Europäischen Kommission bei der Erstellung der Berichte berücksichtigt wird?

Wenn nein, wer unterfällt nach Ansicht der Bundesregierung aus Deutschland dieser Fallgruppe?

Die Bundesregierung wird gegenüber der Europäischen Kommission die Frage aufwerfen, ob im Rahmen von Artikel 97 Absatz 4 der Verordnung (EU) 2016/679 auch Standpunkte oder Feststellungen nationaler Parlamente berücksichtigt werden sollen.

28. Wie wird die Bundesregierung außerhalb der vorgesehenen Berichtszeiträume und der von der Kommission erforderlichenfalls erarbeiteten Änderungsvorschläge dafür Sorge tragen, dass Anpassungen der DSGVO vorgenommen werden können?

Die Bundesregierung plant derzeit keine kurzfristigen Änderungen des schon beschlossenen allgemeinen deutschen Datenschutzrechts und auch keine entsprechende EU-Initiative. In den nächsten Monaten wird es darauf ankommen, Erfahrungen mit dem neuen Recht zu sammeln und sehr genau hinzuschauen, wie die Vorschriften in der Praxis angewandt werden, wie die Verbraucher, die Wirtschaftsunternehmen, die Behörden und die Verbände damit zurechtkommen und welche Belastungen möglicherweise entstehen, um so einen möglichen Anpassungsbedarf zu ermitteln. Ein wichtiger Baustein hierzu ist der Dialog mit der Wirtschaft und den Datenschutzaufsichtsbehörden (vgl. Antwort zu Frage 1).

VI. Betriebliche Datenschutzbeauftragte

29. Wie viele Unternehmen müssen aufgrund der Rechtslage nach Einschätzung der Bundesregierung im Vergleich zur bisherigen Rechtslage ab dem 25. Mai 2018 einen Datenschutzbeauftragten gemäß Artikel 37 DSGVO und § 38 BDSG zusätzlich bestellen?
30. Hat die Bundesregierung Erkenntnisse, welche Kosten den betroffenen Unternehmen hierdurch zusätzlich entstehen?
31. Hat die Bundesregierung Erkenntnisse, welche Kosten deutschen Unternehmen im Vergleich zu Unternehmen in anderen Mitgliedstaaten dadurch entstehen, dass sich der deutsche Gesetzgeber entschieden hat, die Pflicht zur Bestellung eines Datenschutzbeauftragten in § 38 BDSG n. F. auf weitere Fälle auszuweiten?

Die Fragen 29 bis 31 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Der Bundesregierung liegen hierzu keine Erkenntnisse darüber vor, wie viele Unternehmen im Vergleich zur früheren Rechtslage bis zum 24. Mai 2018 einen Datenschutzbeauftragten gemäß Artikel 37 der Verordnung (EU) 2016/679 und § 38 BDSG 2018 einen Datenschutzbeauftragten zusätzlich bestellen müssen, welche Kosten hierfür zusätzlich entstehen und welche Kosten deutschen Unternehmen im Vergleich zu Unternehmen in anderen Mitgliedstaaten aufgrund der Pflicht zur Bestellung eines Datenschutzbeauftragten nach § 38 BDSG 2018 entstehen.

32. Hält die Bundesregierung die Zahl der Personen, die mit der automatisierten Verarbeitung personenbezogener Daten (z. B. Kundendaten in einem Handwerksbetrieb, Geschäft oder Versandhandel) weiterhin für ein sachgerechtes Abgrenzungskriterium?

Die Bundesregierung hält die Zahl der Personen, die mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, als eines von mehreren Abgrenzungskriterien für sachgerecht. Unabhängig davon hat sich die Bundesregierung im Rahmen der nationalen Anpassungsgesetzgebung dafür eingesetzt, die bislang geltenden Voraussetzungen zur Bestellung betrieblicher Datenschutzbeauftragte ergänzend zur Verordnung (EU) 2016/679 zu erhalten. Ziel war es, das Schutzniveau zu erhalten und eine Schwächung des innerbetrieblichen Datenschutzes zu vermeiden.

Im Rahmen der allgemeinen Beobachtungen zur Anwendung der Datenschutz-Grundverordnung (vgl. Antwort zu Frage 28) wird die Bundesregierung die weiteren Entwicklungen zu diesem Institut auch mit Blick auf die fortschreitende Digitalisierung beobachten.

VII. Private Rechtsdurchsetzung

33. Wie viele Einrichtungen, Organisationen oder Vereinigungen in der Bundesrepublik Deutschland erfüllen im Moment die Voraussetzungen, um nach Artikel 82 DSGVO vertreten zu können?

Die Frage wird so verstanden, dass sie sich auf die Vertretung nach Artikel 80 der Verordnung (EU) 2016/679 bezieht. Hierüber hat die Bundesregierung keine Erkenntnisse.

34. Können nach Ansicht der Bundesregierung Verstöße gegen die DSGVO und die ergänzenden Regelungen des BDSG durch einen Wettbewerber oder einen Verband abgemahnt werden, obwohl die DSGVO eine solche Möglichkeit nicht vorsieht?

Handelt es sich bei den Artikeln 77 bis 84 DSGVO um eine abschließende Regelung, welche Abmahnungen durch Wettbewerber anschließt (so etwa Köhler, in: Köhler/Bornkamm/Feddersen, UWG, 36. Auflage 2018, § 3a Rn. 1.40a und 1.74b)?

35. Wenn ja, wird es nach Ansicht der Bundesregierung zu einem Anstieg berechtigter und unberechtigter Abmahnungen durch Wettbewerber oder Verbände kommen?

Wenn ja, mit welchen Kosten für die betroffenen Unternehmen?

Wegen des Sachzusammenhangs werden die Fragen zu 34 und 35 zusammen beantwortet.

Die Verordnung (EU) 2016/679 enthält keine ausdrückliche Aussage darüber, dass Regelungen und Rechtsbehelfe zum Schutz des Wettbewerbs bei Datenschutzverstößen ausgeschlossen werden. Letztlich kann diese Frage jedoch nur durch den EuGH beantwortet werden.

Mitbewerber, klageberechtigte Vereine und Verbände sowie die Industrie- und Handelskammern können auf Grund von § 3a i. V. m. § 8 UWG Verstöße gegen Datenschutzvorschriften abmahnen, soweit diese Vorschriften im Interesse der Marktteilnehmer das Marktverhalten regeln. Bereits im Hinblick auf das bis zum 24. Mai 2018 geltende Datenschutzrecht war die Abmahnfähigkeit von Datenschutzverstößen sehr umstritten, weil Datenschutzvorschriften primär das Persönlichkeitsrecht der Betroffenen schützen.

Zivilrechtliche Unterlassungs- und Beseitigungsansprüche wegen eines Verstoßes gegen datenschutzrechtliche Vorschriften die durch Abmahnungen und Klagen durchsetzbar sind, können sich aus § 2 Absatz 1 des Unterlassungsklagegesetzes (UKlaG) ergeben. Diese Ansprüche stehen den Verbänden und Kammern nach § 3 Absatz 1 Satz 1 UKlaG zu. Wettbewerber sind hiernach nicht klageberechtigt. Nach § 2 Absatz 1 i. V. mit Absatz 2 Satz 1 Nummer 11 UKlaG bestehen Unterlassungsansprüche, wenn Unternehmer datenschutzrechtlichen Vorschriften zuwiderhandeln, die die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von Verbraucherdaten regeln, wenn die Daten zu den Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunft, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben werden. Darunter können auch Vorschriften der Verordnung (EU) 2016/679 und des BDSG 2018 fallen.

36. Plant die Bundesregierung Maßnahmen, um die Folgen von Abmahnungen, insbesondere für kleinere Verstöße ohne direkte Auswirkungen auf die Rechte und Interessen betroffener Personen, zu begrenzen?

Die Bundesregierung nimmt die von Seiten der Unternehmen geäußerten Befürchtungen zu „Abmahnwellen“ im Bereich des Datenschutzes ernst. Im Koalitionsvertrag ist vereinbart, dass ein „Missbrauch des bewährten Abmahnrechts verhindert“ werden soll (Rn. 5819). Gegenwärtig prüft die Bundesregierung Maßnahmen in diesem Bereich.

VIII. Veröffentlichung von Fotografien und Presse

37. Versteht die Bundesregierung Artikel 85 DSGVO als Öffnungsklausel oder als Anpassungsauftrag, und welche Konsequenzen werden aus der entsprechenden Einordnung auch in Bezug auf das KUG gezogen?
38. Stehen nach Ansicht der Bundesregierung die Regelungen zur Veröffentlichung von Bildnissen nach §§ 22 ff. KUG im Einklang mit der DSGVO, soweit deren Anwendungsbereich eröffnet ist?
39. Hält die Bundesregierung es für erforderlich, die §§ 22 ff. KUG aufgrund der Anwendbarkeit der DSGVO anzupassen?
Wenn ja, welche Anpassung plant die Bundesregierung, und wann soll sie erfolgen?
40. Ist die Bundesregierung der Ansicht, dass die §§ 22 ff. KUG erhalten werden können oder sogar müssen, um das Recht auf Datenschutz mit der Meinungsfreiheit und Informationsfreiheit in Einklang zu bringen?
41. Sieht die Bundesregierung auch eine Möglichkeit zum Erhalt der §§ 22 ff. KUG, soweit mit der Veröffentlichung eines Bildnisses keine Meinungsäußerung verbunden ist?
42. Welche Regelungen sind nach Ansicht der Bundesregierung ab dem 25. Mai 2018 auf die Verarbeitung (Artikel 4 Nummer 1 DSGVO) von Abbildungen (z. B. deren Erhebung und Speicherung) anwendbar, die vor einer Verbreitung oder öffentlichen Zurschaustellung des Bildnisses erfolgt?
43. Erfordert nach Ansicht der Bundesregierung ab dem 25. Mai 2018 die Veröffentlichung jeder Fotografie, die in den Anwendungsbereich der DSGVO fällt, eine Einwilligung?
44. Welche Unterschiede ergeben sich nach Ansicht der Bundesregierung, wenn eine Veröffentlichung von Fotografien, die in den Anwendungsbereich der DSGVO fällt, nicht mehr nach §§ 22, 23 KUG zu beurteilen wäre, sondern nach Artikel 6 DSGVO?
Wird sich nach Ansicht der Bundesregierung die Rechtslage ändern, wenn statt der typisierten Interessenabwägung des § 23 KUG nunmehr die offene Interessenabwägung des Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO zur Anwendung kommt?
45. Richtete sich die Verarbeitung von Fotografien, die in den Anwendungsbereich des BDSG oder der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, bis zum 25. Mai 2018 nach den Regelungen des KUG oder den datenschutzrechtlichen Vorschriften?
Standen die §§ 22 ff. KUG im Einklang mit der Richtlinie 95/46/EG, insbesondere im Hinblick auf die Anforderungen an die Einwilligung und die fehlende offene Abwägung der Interessen im Rahmen des § 23 KUG?

Die Fragen 37 und 45 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Die Verordnung (EU) 2016/679 führt zu keinen wesentlichen Veränderungen der bisherigen Rechtslage im Umgang mit Fotografien. Die Anfertigung und Veröffentlichung einer personenbezogenen Fotografie unterliegt den allgemeinen Regelungen des Datenschutzrechts. Wie bisher auch dürfen Fotos nur verarbeitet werden, wenn die betroffene Person eingewilligt hat oder eine Rechtsgrundlage dies erlaubt.

Erfolgt die Anfertigung auf der Grundlage einer Einwilligung der betroffenen Person(en), ist diese bereits nach geltendem Recht jederzeit widerrufbar. Aufgrund der jederzeitigen Widerruflichkeit und der fehlenden Praktikabilität bei Aufnahmen größerer Menschenmengen ist die datenschutzrechtliche Einwilligung bereits nach geltender Rechtslage vielfach keine praktikable Rechtsgrundlage.

Neben der Einwilligung kommen als weitere Rechtsgrundlagen für die Anfertigung und Veröffentlichung zur Durchführung eines Vertrags (Artikel 6 Absatz 1 Buchstabe b) Verordnung (EU) 2016/679) oder zur Wahrnehmung berechtigter Interessen des Fotografen (Artikel 6 Absatz 1 Buchstabe f) Verordnung (EU) 2016/679) in Betracht.

Die grundrechtlich geschützte und garantierte Meinungs- und Informationsfreiheit stellen berechnigte Interessen nach Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 dar. Sie fließen somit unmittelbar in die Auslegung und Anwendung der Datenschutz-Grundverordnung ein. Die Datenschutz-Grundverordnung betont, dass der Schutz personenbezogener Daten kein uneingeschränktes Recht ist, sondern im Hinblick auf seine gesellschaftliche Funktion und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss (Erwägungsgrund 4).

Für die Veröffentlichung von Fotografien enthält das Kunsturhebergesetz (KunstUrhG) ergänzende Regelungen, die auch unter der ab dem 25. Mai 2018 anwendbaren Datenschutz-Grundverordnung fortbestehen. Das Kunsturhebergesetz stützt sich auf Artikel 85 Absatz 1 der Verordnung (EU) 2016/679, der den Mitgliedstaaten nationale Gestaltungsspielräume bei dem Ausgleich zwischen Datenschutz und der Meinungs- und Informationsfreiheit eröffnet. Es steht nicht im Widerspruch zur Datenschutz-Grundverordnung, sondern fügt sich als Teil der deutschen Anpassungsgesetzgebung in das System der Datenschutz-Grundverordnung ein.

IX. Medienprivileg sowie Meinungs- und Informationsfreiheit

46. Plant die Bundesregierung auf Basis von Artikel 85 Absatz 1 DSGVO weitere gesetzgeberische Maßnahmen, um Meinungs- und Informationsfreiheit mit dem Recht auf Datenschutz in Ausgleich zu bringen?

Die Bundesregierung plant derzeit keine weiteren gesetzgeberischen Maßnahmen mit Blick auf Artikel 85 Absatz 1 der Verordnung (EU) 2016/679. Im Rahmen der allgemeinen Beobachtungen zur Anwendung der Datenschutz-Grundverordnung (vgl. Antwort zu Frage 28) wird die Bundesregierung auch hierzu die weiteren Entwicklungen und praktischen Erfahrungen beobachten.

47. Verfügt der Bund nach Ansicht der Bundesregierung über die Gesetzgebungskompetenz, um die Verarbeitung von personenbezogenen Daten durch die Presse gemäß Artikel 85 Absatz 2 DSGVO von der Anwendung von Teilen der DSGVO auszunehmen?

Wäre aus Sicht der Bundesregierung eine bundeseinheitliche Regelung – auch im Hinblick auf Presseveröffentlichungen im Internet – wünschenswert?

Der Bund ist nach der Föderalismusreform II nur noch zuständig für die Regelungen im Zusammenhang mit der „Deutschen Welle“. Die ausschließliche Gesetzgebungskompetenz des Bundes für den Erlass von Regelungen zur Deutschen Welle im Deutsche Welle Gesetz ergibt sich aus der Kompetenz des Bundes für

„Auswärtige Angelegenheiten“ aus den Artikeln 32 und 73 Absatz 1 Nummer 1 des Grundgesetzes. Die Anpassung des Deutschen-Welle-Gesetzes unter Nutzung der Öffnungsklausel Artikel 85 Verordnung (EU) 2016/679 ist Gegenstand des 2. Datenschutz- Anpassungs- und Umsetzungsgesetz EU (sog. „Omnibus-Gesetz“).

Im Übrigen sind infolge der Föderalismusreform II die Länder zuständig, welche u. a. mit den entsprechenden Landespressegesetzen und dem Rundfunkstaatsvertrag das Medienprivileg schützen.

48. Welche Anforderungen muss eine Aufsichtsbehörde über die Datenverarbeitung zu journalistischen Zwecken erfüllen, damit insbesondere das Recht auf eine wirksame Beschwerde nach Artikel 77 Absatz 1 DSGVO gewährleistet bleibt, da Artikel 85 Absatz 2 DSGVO keinen Dispens von Kapitel VIII der DSGVO vorsieht?

Über welche Befugnisse und Sanktionsmöglichkeiten muss eine solche Aufsichtsbehörde verfügen, damit sie einer Beschwerde wirksam abhelfen kann?

Kann eine solche Aufsichtsbehörde nach Ansicht der Bundesregierung nur auf gesetzlicher Grundlage eingerichtet werden oder ist eine Aufsicht im Wege der Selbstregulierung möglich?

Artikel 85 Absatz 1 der Verordnung (EU) 2016/679 ist als zentraler Regelungsauftrag an die Mitgliedstaaten konzipiert, nach dem Prinzip der praktischen Konkordanz einen angemessenen Ausgleich zwischen den Grundrechten auf Meinungs- und Informationsfreiheit und dem Recht auf den Schutz personenbezogener Daten zu finden.

Die Wahl der Mittel und die konkrete Regelung obliegen den Mitgliedstaaten und erlauben umfassende Einschränkungen inklusive des Kapitels VIII Verordnung (EU) 2016/679.

Hinsichtlich der Regelungen im Zusammenhang mit der „Deutschen Welle“, für die der Bund zuständig ist, ist angedacht, um der verfassungsrechtlich gewährleisteten Rundfunkfreiheit einerseits und den Anforderungen des Datenschutzes andererseits gerecht zu werden, eine Beauftragte oder ein Beauftragter für den Datenschutz als zuständige Aufsichtsbehörde für die Datenverarbeitung im journalistischen Bereich vorzusehen. Diese oder dieser tritt dann im Bereich der Datenverarbeitung zu journalistischen Zwecken an die Stelle der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Der oder dem Beauftragten für den Datenschutz sollen als Aufsichtsbehörde die in den Kapiteln VI und VII der Verordnung (EU) 2016/679 genannten Aufgaben und Befugnisse zustehen, soweit nicht abweichende Regelungen getroffen werden. Kapitel VIII der Verordnung (EU) 2016/679 soll unmittelbar gelten. Hierbei ist aber zu berücksichtigen, dass die „Deutsche Welle“ nur bestimmte datenschutzrechtliche Pflichten überhaupt treffen können (Artikel 5 Absatz 1 Buchstabe f), Artikel 24, Artikel 32 der Verordnung (EU) 2016/679).

Die Errichtung einer Datenschutzaufsichtsbehörde muss eine Grundlage im nationalen Recht haben. Der EU-Gesetzgeber hat verdeutlicht, dass es aber nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt bedarf (Erwägungsgrund 41 Satz 1).

49. Ist nach Ansicht der Bundesregierung eine generelle Privilegierung der Meinungsfreiheit gegenüber der DSGVO ähnlich dem schwedischen Modell („Die EU-Datenschutz-Grundverordnung sowie weitere Datenschutzgesetze finden in dem Umfang, wie sie gegen Presse- oder Meinungsfreiheit streiten, keine Anwendung.“) mit dem Unionsrecht vereinbar?

Wenn ja, wie beurteilt die Bundesregierung eine solche Regelung mit Blick auf Deutschland?

Wenn nein, weshalb nicht, und strebt Deutschland dann ein Vertragsverletzungsverfahren gegen Schweden an?

Ist der Bundesregierung die Haltung der Europäischen Kommission zu dieser Regelung bekannt?

Der schwedische Ansatz bringt nach Ansicht der Bundesregierung keine Rechtssicherheit. Fälle, in denen verschiedene Grundfreiheiten sich Streitgegenständlich gegenüber stehen, sollten und können auch im Datenschutzrecht nach den allgemeinen Kollisionsregeln gelöst werden. Dies verdeutlicht der EU-Gesetzgeber auch am Erwägungsgrund 4 Satz 2 Verordnung (EU) 2016/679.

Die Bundesregierung sieht derzeit keinen Anlass für eine Vertragsverletzungsklage nach Artikel 259 AEUV gegen Schweden.

Die Haltung der Europäischen Kommission zu dieser Frage ist nicht bekannt.

