Freitag, 21. Mai 2021

P9_TA(2021)0262

Der angemessene Schutz personenbezogener Daten vonseiten des Vereinigten Königreichs

Entschließung des Europäischen Parlaments vom 21. Mai 2021 zu der Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (2021/2594(RSP))

(2022/C 15/23)

Das Europäische Parlament,

— unter Hinweis auf die Charta der Grundrechte der Europäischen Union (Charta), insbesondere auf Artikel 7, 8, 16, 47 und 52,

— unter Hinweis auf das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner/Facebook Ireland Limited und Maximillian Schrems („Schrems II“) ([1]),

— unter Hinweis auf das Urteil des EuGH vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems I“) ([2]),

— unter Hinweis auf das Urteil des EuGH vom 6. Oktober 2020 in der Rechtssache C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs ([3]),

— unter Hinweis auf seine Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres ([4]),

— unter Hinweis auf seine Entschließung vom 5. Juli 2018 zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes ([5]),

— unter Hinweis auf seine Entschließung vom 25. Oktober 2018 zu der Nutzung der Daten von Facebook-Nutzern durch Cambridge Analytica und den Auswirkungen auf den Datenschutz ([6]),

— unter Hinweis auf seine Entschließung vom 20. Mai 2021 zu dem Urteil des EuGH vom 16. Juli 2020 — Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems („Schrems II“) — Rechtssache C-311/18 ([7]),

— unter Hinweis auf seine Entschließung vom 26. November 2020 zur Überprüfung der Handelspolitik der EU ([8]),

— unter Hinweis auf das Handels- und Kooperationsabkommen vom 31. Dezember 2020 zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits ([9]),

— unter Hinweis auf seine Entschließung vom 28. April 2021 zum Ergebnis der Verhandlungen zwischen der EU und dem Vereinigten Königreich ([10]),

— unter Hinweis auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) ([11]) (DSGVO),

---

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) ABl. C 378 vom 9.11.2017, S. 104.
([5]) ABl. C 118 vom 8.4.2020, S. 133.
([6]) ABl. C 345 vom 16.10.2020, S. 58.
([7]) Angenommene Texte, P9_TA(2021)0256.
([8]) Angenommene Texte, P9_TA(2020)0337.
([9]) ABl. L 444 vom 31.12.2020, S. 14.
([10]) Angenommene Texte, P9_TA(2021)0141.
([11]) ABl. L 119 vom 4.5.2016, S. 1.

— unter Hinweis auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr ([12]) (Richtlinie zum Datenschutz bei der Strafverfolgung),

— unter Hinweis auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation ([13]),

— unter Hinweis auf den Vorschlag der Kommission vom 10. Januar 2017 für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (COM(2017)0010) und die dazu am 20. Oktober 2017 angenommene Stellungnahme des Europäischen Parlaments ([14]),

— unter Hinweis auf die Empfehlungen des Europäischen Datenschutzausschusses (EDSA), einschließlich seiner Erklärung vom 9. März 2021 zur ePrivacy-Verordnung und seiner Empfehlungen 01/2020 vom 10. November 2020 zu Maßnahmen, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Datenschutzniveaus zu gewährleisten,

— unter Hinweis auf die von der Artikel 29 Datenschutzgruppe am 6. Februar 2018 angenommene und vom EDSA gebilligte Referenzgrundlage für Angemessenheit,

— unter Hinweis auf die Empfehlungen 01/2021 des EDSA vom 2. Februar 2021 zu der Referenzgrundlage für Angemessenheit im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung,

— unter Hinweis auf die von der Kommission am 19. Februar 2021 veröffentlichten Entwürfe zu Angemessenheitsbeschlüssen, einer gemäß der DSGVO ([15]) und der andere gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung ([16]),

— unter Hinweis auf die Stellungnahmen 14/2021 und 15/2021 des EDSA vom 13. April 2021 zu dem Entwurf eines Durchführungsbeschlusses der Kommission gemäß der Richtlinie (EU) 2016/680 zu der Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich,

— unter Hinweis auf die Europäische Menschenrechtskonvention (EMRK) und das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sowie das dazugehörige Änderungsprotokoll („Übereinkommen Nr. 108+“), bei denen das Vereinigte Königreich Vertragspartei ist,

— unter Hinweis auf die Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren,

— gestützt auf Artikel 132 Absatz 2 seiner Geschäftsordnung,

— unter Hinweis auf den Entschließungsantrag des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres,

A. in der Erwägung, dass die Möglichkeit, personenbezogene Daten über Grenzen hinweg zu übermitteln, ein treibender Motor für Innovation, Produktivität und wirtschaftliche Wettbewerbsfähigkeit sein kann und entscheidend für eine wirksame Zusammenarbeit bei der Bekämpfung von grenzübergreifender organisierter und schwerer Kriminalität sowie von Terrorismus ist, der zunehmend vom Austausch personenbezogener Daten abhängt;

B. in der Erwägung, dass der EuGH in seinem Urteil in der Rechtssache Schrems I darauf hingewiesen hat, dass ein willkürlicher Zugriff der Geheimdienste auf den Inhalt elektronischer Kommunikation eine Verletzung des Wesensgehalts des in Artikel 7 der Charta der Grundrechte der Europäischen Union vorgesehenen Rechts auf Vertraulichkeit der Kommunikation darstellt und dass die Vereinigten Staaten keine hinreichenden Rechtsbehelfe für Nicht-US-Bürger gegen die Massenüberwachung vorsehen, was eine Verletzung von Artikel 47 der Charta darstellt;

([12]) ABl. L 119 vom 4.5.2016, S. 89.
([13]) ABl. L 201 vom 31.7.2002, S. 37.
([14]) A8-0324/2017.
([15]) Entwurf eines Durchführungsbeschlusses der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum angemessenen Schutz personenbezogener Daten durch das Vereinigte Königreich.
([16]) Entwurf eines Durchführungsbeschlusses der Kommission gemäß der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zum angemessenen Schutz personenbezogener Daten durch das Vereinigte Königreich,

C. in der Erwägung, dass das Vereinigte Königreich seit jeher ein wichtiger Handelspartner vieler EU-Mitgliedstaaten sowie ein enger Verbündeter im Bereich der Sicherheit ist; in der Erwägung, dass die EU und das Vereinigte Königreich diese enge Zusammenarbeit trotz des Austritts des Vereinigten Königreichs aus der EU aufrechterhalten sollten, da dies für beide Seiten von Vorteil sein würde;

D. in der Erwägung, dass europäische Unternehmen Rechtsklarheit und Rechtssicherheit benötigen, da die Möglichkeit, personenbezogene Daten über Grenzen hinweg zu übermitteln, für alle Arten von Unternehmen, die international Waren und Dienstleistungen anbieten, zunehmend an Bedeutung gewonnen hat; in der Erwägung, dass ein Angemessenheitsbeschluss bezüglich des Vereinigten Königreichs im Rahmen der DSGVO von größter Bedeutung ist, da viele europäische Unternehmen Handel über den Ärmelkanal betreiben, insbesondere angesichts der Tatsache, dass der Brexit erst vor kurzem erfolgt ist und der Datenverkehr innerhalb der Union keinen Beschränkungen unterliegt; in der Erwägung, dass ohne einen soliden Angemessenheitsrahmen die Gefahr von Störungen bei der grenzübergreifenden Übermittlung personenbezogener Daten zwischen der EU und dem Vereinigten Königreich zu Geschäftszwecken sowie von hohen Befolgungskosten besteht;

E. in der Erwägung, dass das Handels- und Kooperationsabkommen eine Reihe von Garantien und Bedingungen für den Austausch relevanter personenbezogener Daten im Rahmen der Strafverfolgung enthält; in der Erwägung, dass die Verhandlungen über den Verkehr personenbezogener Daten parallel zu den Verhandlungen über das Handels- und Kooperationsabkommen geführt wurden, bis zum Ende des Übergangszeitraums am 31. Dezember 2020 jedoch noch nicht abgeschlossen waren; in der Erwägung, dass eine „Überbrückungsklausel" als Zwischenlösung in das Handels- und Kooperationsabkommen aufgenommen wurde, die von der Zusage des Vereinigten Königreichs abhängig gemacht wurde, seine derzeitige Datenschutzregelung nicht zu ändern, damit die Fortsetzung des Verkehrs personenbezogener Daten zwischen dem Vereinigten Königreich und der EU bis zur Annahme eines Angemessenheitsbeschlusses sichergestellt ist; in der Erwägung, dass der ursprüngliche Zeitraum von vier Monaten verlängert wurde und Ende Juni 2021 ausläuft;

F. in der Erwägung, dass die Bewertung, die die Kommission vor der Vorlage ihres Entwurfs eines Durchführungsbeschlusses vorgenommen hat, unvollständig ist und nicht mit den Anforderungen des EuGH an Angemessenheitsbewertungen im Einklang steht, worauf der EDSA in seinen Stellungnahmen zur Angemessenheit hingewiesen hat, in denen er der Kommission empfiehlt, bestimmte Aspekte des Rechts und der Vorgehensweise des Vereinigten Königreichs in Bezug auf Sammelerhebungen, die Offenlegung im Ausland und internationale Abkommen im Bereich des Austauschs nachrichtendienstlicher Erkenntnisse, die zusätzliche Nutzung der für Strafverfolgungszwecke gesammelten Informationen und die Unabhängigkeit der Justizkommissare weiter zu prüfen;

G. in der Erwägung, dass bestimmte Aspekte des Rechts bzw. der Praxis des Vereinigten Königreichs von der Kommission nicht berücksichtigt wurden, was zu Entwürfen von Durchführungsbeschlüssen geführt hat, die mit dem Unionsrecht unvereinbar sind; in der Erwägung, dass Artikel 45 DSGVO besagt, dass die Kommission bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus insbesondere das Folgende berücksichtigen muss: „die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art — auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten — sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung" und „die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben", was auch internationale Übereinkünfte in anderen Bereichen einschließt, die einen Zugang zu Daten oder einen Informationsaustausch umfassen, sodass eine Bewertung solcher internationalen Übereinkünfte erforderlich ist;

H. in der Erwägung, dass der EuGH in seiner Entscheidung in der Rechtssache Schrems I ganz klar ausführt, dass die Kommission unter diesen Umständen „bei der Prüfung des von einem Drittland gebotenen Schutzniveaus verpflichtet [ist], den Inhalt der in diesem Land geltenden, aus seinen innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen resultierenden Regeln sowie die zur Gewährleistung der Einhaltung dieser Regeln dienende Praxis zu beurteilen, wobei sie nach Art. 25 Abs. 2 der Richtlinie 95/46/EG alle Umstände zu berücksichtigen hat, die bei einer Übermittlung personenbezogener Daten in ein Drittland eine Rolle spielen" (Rn. 75);

I. in der Erwägung, dass die Tätigkeiten der Nachrichtendienste und der Austausch mit Drittländern vom Anwendungsbereich der Rechtsvorschriften der EU aufgrund der Verträge ausgeschlossen sind, was die Mitgliedstaaten betrifft, da sie Gegenstand der notwendigen Abschätzung der Angemessenheit des von Drittländern gebotenen Niveaus des Schutzes personenbezogener Daten sind, wie der EuGH in den Urteilen „Schrems I" und „Schrems II" bestätigt hat;

J. in der Erwägung, dass sich die Datenschutzstandards nicht nur auf die geltenden Rechtsvorschriften, sondern auch auf deren Anwendung in der Praxis stützen, und in der Erwägung, dass die Kommission bei der Vorbereitung ihrer Entscheidung lediglich die Rechtsvorschriften, nicht aber ihre tatsächliche Anwendung in der Praxis bewertet hat;

K. in der Erwägung, dass die Kommission derzeit zwölf Drittländer anerkennt, deren Schutz im Rahmen der DSGVO angemessen ist, und vor kurzem diesbezügliche Gespräche mit der Republik Korea abgeschlossen hat; in der Erwägung, dass das Vereinigte Königreich das erste Land ist, für das die Kommission vorgeschlagen hat, Angemessenheit im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung zu gewähren;

L. in der Erwägung, dass sich der Fall des Vereinigten Königreichs von allen bisherigen Angemessenheitsbewertungen unterscheidet, da er einen ehemaligen EU-Mitgliedstaat betrifft, der die Bestimmungen der DSGVO in sein nationales Recht übernommen und darüber hinaus festgelegt hat, dass alle „von der EU abgeleiteten innerstaatlichen Rechtsvorschriften", einschließlich der Rechtsvorschriften zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung, auch nach dem Ende des Übergangszeitraums weiterhin gelten werden;

I. **DATENSCHUTZ-GRUNDVERORDNUNG**

Allgemeine Bemerkungen

1. weist darauf hin, dass das Vereinigte Königreich zu den Unterzeichnern der Europäischen Menschenrechtskonvention (EMRK) und des Übereinkommens des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten gehört; erwartet, dass das Vereinigte Königreich den gleichen Mindestrahmen für den Datenschutz gewährleistet, auch wenn es die Europäische Union verlassen hat;

2. begrüßt das Bekenntnis des Vereinigten Königreichs, Demokratie und Rechtsstaatlichkeit zu achten und Grundrechte, wie sie etwa in der EMRK verankert sind, zu schützen und innenpolitisch umzusetzen, was ein hohes Datenschutzniveau einschließt; weist erneut darauf hin, dass dies eine erforderliche Bedingung für die Zusammenarbeit der EU mit dem Vereinigten Königreich ist; weist darauf hin, dass Artikel 8 EMRK zum Recht auf Privatsphäre zwar über den Human Rights Act 1998 (Gesetz über Menschenrechte) Teil des innerstaatlichen Rechts und über das neue Delikt der missbräuchlichen Verwendung von Datenschutzinformationen Teil des Gewohnheitsrechts des Vereinigten Königreichs ist, aber Bemühungen um die Aufnahme eines Grundrechts auf Datenschutz von der Regierung abgelehnt wurden;

3. weist darauf hin, dass sich die EU bei der Entwicklung robuster Datenschutzvorschriften im Rahmen der DSGVO für einen menschenrechtsorientierten Ansatz bei der Daten-Governance entschieden hat, und ist daher zutiefst besorgt über öffentliche Erklärungen des britischen Premierministers, der verkündet hat, das Vereinigte Königreich wolle sich von den EU-Datenschutzvorschriften lossagen und eigene „souveräne" Regelungen in diesem Bereich einführen; ist der Auffassung, dass die Nationale Datenstrategie des Vereinigten Königreichs von 2020 eine Abwendung vom Schutz personenbezogener Daten hin zu einer breiteren Nutzung und Weitergabe von Daten darstellt, die mit den Grundsätzen der Rechtmäßigkeit, Datenminimierung und Zweckbindung gemäß DSGVO unvereinbar ist; weist darauf hin, dass der EDSA in seinen Angemessenheitsbewertungen betont hat, dass dies zu möglichen Risiken in Bezug auf den Schutz personenbezogener Daten, die aus der EU übermittelt werden, führen könnte;

4. weist darauf hin, dass gültige Angemessenheitsbeschlüsse erheblich zum Schutz der Grundrechte von Einzelpersonen und zur Rechtssicherheit für Unternehmen beitragen; betont jedoch, dass Angemessenheitsbeschlüsse, die auf unvollständigen Bewertungen beruhen und von der Kommission nicht ordnungsgemäß durchgesetzt werden, das Gegenteil bewirken können, wenn sie vor Gericht angefochten werden;

5. weist darauf hin, dass die Bewertung, die die Kommission vor der Vorlage ihres Entwurfs eines Durchführungsbeschlusses vorgenommen hat, unvollständig ist und nicht mit den Anforderungen des EuGH für Angemessenheitsbewertungen im Einklang steht, worauf der EDSA in seinen Stellungnahmen zur Angemessenheit hingewiesen hat, in denen er der Kommission empfiehlt, bestimmte Elemente des Rechts oder der Vorgehensweise des Vereinigten Königreichs in Bezug auf Sammelerhebungen, die Offenlegung im Ausland und internationale Abkommen im Bereich des Austauschs nachrichtendienstlicher Erkenntnisse, die zusätzliche Nutzung der für Strafverfolgungszwecke gesammelten Informationen und die Unabhängigkeit der Justizkommissare weiter zu prüfen;

Durchsetzung der DSGVO

6. äußert seine Besorgnis über die mangelnde und oftmals ganz unterbliebene Durchsetzung der DSGVO durch das Vereinigte Königreich, als es noch Mitglied der EU war; verweist insbesondere auf die unzureichende Durchsetzung durch das Amt des Datenschutzbeauftragten des Vereinigten Königreichs in der Vergangenheit; weist auf das Beispiel des Amtes des britischen Datenschutzbeauftragten hin, das nach zwei Veranstaltungen mit Interessenträgern eine Beschwerde bezüglich Adtech abgeschlossen, einen Bericht („Update Report on Adtech") erstellt und erklärt hat, dass die Adtech-Branche in Bezug auf ihr Verständnis der Datenschutzanforderungen unausgereift erscheine, jedoch von keiner ihrer

Durchsetzungsbefugnisse Gebrauch gemacht hat ([17]); ist besorgt darüber, dass die fehlende Durchsetzung ein strukturelles Problem ist, das in den Leitlinien des Amtes des britischen Datenschutzbeauftragten für Regulierungsmaßnahmen festgeschrieben ist, wo es ausdrücklich heißt, dass das Amt seine Befugnisse ausschließlich in den schwerwiegendsten Fällen, die die gröbsten Verstöße gegen die Informationspflichten darstellten und bei denen es sich in der Regel um vorsätzliche, bewusste oder fahrlässige Handlungen oder um wiederholte Verstöße gegen Informationspflichten handele, durch die Einzelpersonen Personen- oder Sachschäden zugefügt würden, wahrnehmen werde; betont, dass dies in der Praxis dazu geführt hat, dass zahlreiche Verstöße gegen das Datenschutzrecht im Vereinigten Königreich nicht abgestellt worden sind;

7. nimmt die am 9 Dezember 2020 aktualisierte nationale Datenstrategie des Vereinigten Königreichs zur Kenntnis, die auf eine Abwendung vom Schutz personenbezogener Daten hin zu einer verstärkten und breiteren Nutzung und Weitergabe von Daten hindeutet; weist darauf hin, dass das „Zurückhalten von Daten", wie in der Strategie erwähnt, negative Auswirkungen auf die Gesellschaft haben kann und nicht mit den Grundsätzen der Datensparsamkeit und der Zweckbindung gemäß der DSGVO und dem Primärrecht vereinbar ist;

8. nimmt zur Kenntnis, dass der Ausschuss für konstitutionelle Fragen des britischen Parlaments im Jahr 2004 ([18]) und sein Ausschuss für öffentliche Angelegenheiten im Jahr 2014 ([19]) empfohlen haben, die Unabhängigkeit Amtes des britischen Datenschutzbeauftragten sicherzustellen, indem der Datenschutzbeauftragte den Status eines Beamten des Parlaments erhält, der dem Parlament unterstellt ist und nicht mehr vom Minister für Digitales, Kultur, Medien und Sport ernannt wird; bedauert, dass diese Empfehlung nicht umgesetzt wurde;

Datenverarbeitung für die Einwanderungskontrolle

9. weist darauf hin, dass das Datenschutzrecht des Vereinigten Königreichs eine Ausnahmeregelung zu bestimmten Aspekten der grundlegenden Datenschutzrechte und -grundsätze beinhaltet, beispielsweise zum Recht auf Auskunft und zum Recht einer betroffenen Person, zu erfahren, an wen ihre Daten weitergegeben werden, wenn eine wirksame Einwanderungskontrolle durch einen solchen Schutz beeinträchtigt würde; betont, dass die Überwachung und die Einhaltung der Ausnahmeregelung im Einklang mit den in der Referenzgrundlage für Angemessenheit vorgesehenen Standards erfolgen müssen, was eine Betrachtung sowohl der Praxis als auch des Prinzips erfordert, indem darauf hingewiesen wird, dass nicht nur die Vorschriften für personenbezogene Daten, die in ein Drittland übermittelt werden, an sich, sondern auch das bestehende System zur Gewährleistung der Wirksamkeit solcher Vorschriften berücksichtigt werden müssen; erkennt an, dass diese Ausnahmeregelung, die von allen für die Verarbeitung Verantwortlichen im Vereinigten Königreich in Anspruch genommen werden kann, vom ICO und einem Gericht gebilligt wurde und nur im Einzelfall geltend gemacht und auf notwendige und verhältnismäßige Weise angewandt werden kann; weist auf kürzlich bekannt gewordene Informationen hin, wonach 17 780 Auskunftsersuchen zu Daten, die zwischen dem 1. April 2018 und dem 31. März 2019 vom Innenministerium verarbeitet wurden, in Bezug auf 146,75 Millionen betroffene Personen gestellt wurden und die Ausnahmeregelung für die Einwanderung im Jahr 2020 bei mehr als 70 % der Anfragen betroffener Personen an das Innenministerium zur Anwendung kam ([20]); betont, dass selbst in den Fällen, in denen das Innenministerium von der Ausnahmeregelung Gebrauch machte, der Zugang zu Informationen nicht vollständig verweigert, sondern auf geschwärzte Dokumente beschränkt wurde;

10. weist darauf hin, dass diese Ausnahmeregelung jetzt für EU-Bürger gilt, die im Vereinigten Königreich wohnen oder wohnen wollen; ist zutiefst besorgt darüber, dass durch die Ausnahmeregelung wesentliche Möglichkeiten zur Sicherstellung der Rechenschaftspflicht und für Rechtsbehelfe beseitigt werden, und betont, dass dies kein angemessenes Schutzniveau ist;

([17]) Lomas, N., *UK's ICO faces legal action after closing adtech complaint with nothing to show for it* (Rechtliche Schritte gegen das Amt des Datenschutzbeauftragten des Vereinigten Königreichs nach ergebnisloser Einstellung der Bearbeitung der Beschwerde über die Adtech-Branche), TechCrunch, San Francisco, 2020.

([18]) Siebter Bericht des Sonderausschusses für konstitutionelle Fragen, veröffentlicht vom britischen Unterhaus am 13. Juni 2006. Dort heißt es unter Ziffer 108: „We see considerable merit in the Information Commissioner becoming directly responsible to, and funded by, Parliament, and recommend that such a change be considered when an opportunity arises to amend the legislation." (Wir sehen beträchtliche Vorteile darin, dass der Datenschutzbeauftragte direkt dem Parlament unterstellt und von diesem finanziert wird, und empfehlen, eine solche Änderung in Betracht zu ziehen, wenn sich eine Gelegenheit zur Änderung der Rechtsvorschriften ergibt.).

([19]) Bericht des Ausschusses für öffentliche Verwaltung mit dem Titel „Who's accountable? Relationships between Government and arm's-length bodies" (Wer ist rechenschaftspflichtig? Beziehungen zwischen der Regierung und unabhängigen Stellen), veröffentlicht vom Unterhaus am 4. November 2014. Dort heißt es unter Ziffer 64: „The Information Commissioner and HM Inspectorate of Prisons should be more fully independent of Government and should report to Parliament. The Information Commissioner, Commissioner for Public Appointments and the Chair of the Committee on Standards in Public Life should become Officers of Parliament, as the Parliamentary and Health Service Ombudsman and the Comptroller and Auditor General already are." (Der Datenschutzbeauftragte und die königliche Strafvollzugsbehörde sollten unabhängiger von der Regierung und dem Parlament unterstellt sein. Der Datenschutzbeauftragte, der Beauftragte für Ernennungen im öffentlichen Dienst und der Vorsitzende des Ausschusses für Verhaltensregeln im öffentlichen Dienst sollten Beamte des Parlaments werden, wie es der Bürgerbeauftragte für das Parlament und den Gesundheitsdienst und der Vorsitzende des Rechnungshofs bereits sind.).

([20]) Open Rights Group, Presseveröffentlichung vom 3. März 2021 mit dem Titel „Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office" (Dokumente offenbaren Anwendung der umstrittenen Ausnahmeregelung für die Einwanderung bei 70 % der Anträge auf Auskunft).

11. bekräftigt seine ernsthaften Bedenken hinsichtlich der Ausnahmeregelung bezüglich der Rechte betroffener Personen in der Einwanderungspolitik des Vereinigten Königreichs; bekräftigt seinen Standpunkt, dass die im britischen Data Protection Act (Datenschutzgesetz) vorgesehene Ausnahme bezüglich der für Einwanderungszwecke vorgenommenen Verarbeitung personenbezogener Daten geändert werden muss, bevor eine stichhaltige Entscheidung über die Angemessenheit getroffen werden kann, wie es bereits wiederholt zum Ausdruck gebracht hat, unter anderem in seiner Entschließung vom 12. Februar 2020 zu dem vorgeschlagenen Mandat für die Verhandlungen über eine neue Partnerschaft mit dem Vereinigten Königreich Großbritannien und Nordirland ([21]) und in der Stellungnahme des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres vom 5. Februar 2021 ([22]); fordert die Kommission auf, die Aufhebung der Ausnahmeregelung für die Einwanderung anzustreben oder dafür zu sorgen, dass sie so geändert wird, dass den betroffenen Personen im Rahmen der Ausnahme und ihrer Anwendung ausreichende Garantien geboten werden und mit ihnen nicht gegen die von einem Drittland erwarteten Standards verstoßen wird;

Massenüberwachung

12. weist erneut auf die Enthüllungen des Hinweisgebers Edward Snowden zur Massenüberwachung durch die USA und das Vereinigte Königreich hin; verweist darauf, dass das britische Programm „Tempora" der Kommunikationszentrale der Regierung des Vereinigten Königreichs (Government Communications Headquarters, GCHQ) Datenverkehr über Internet-Backbone-Glasfaserkabel in Echtzeit abfängt und die Daten speichert, sodass sie zu einem späteren Zeitpunkt verarbeitet und durchsucht werden können; weist darauf hin, dass diese Massenüberwachung von Datenverkehrsinhalten und Metadaten unabhängig davon durchgeführt wird, ob es einen konkreten Verdacht gibt oder ob bestimmte Daten gesucht werden;

13. weist erneut darauf hin, dass der EuGH in den Urteilen zu den Rechtssachen „Schrems I" und „Schrems II" entschieden hat, dass der massenhafte Zugriff auf die Inhalte privaten Datenverkehrs den Wesensgehalt des Rechts auf Privatsphäre berührt und dass in solchen Fällen eine Prüfung der Notwendigkeit und Verhältnismäßigkeit nicht mehr erforderlich ist; betont, dass diese Grundsätze für Datenübertragungen in andere Drittländer als die USA, einschließlich des Vereinigten Königreichs, gelten;

14. weist erneut auf seine Entschließung vom 12. März 2014 hin, in der es festgestellt hat, dass wahllos und ohne Vorliegen eines Verdachts durchgeführte Massenüberwachungsprogramme des britischen Nachrichtendienstes GCHQ mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit in einer demokratischen Gesellschaft unvereinbar und nach Datenschutzrecht der EU unverhältnismäßig sind; erkennt an, dass das Vereinigte Königreich seine Überwachungsgesetze seither erheblich reformiert und Schutzmechanismen eingeführt hat, die über die vom Gerichtshof der Europäischen Union (EuGH) in seinem Urteil in der Rechtssache „Schrems II" ([23]) festgelegten Bedingungen sowie über die Garantien hinausgehen, die in den Überwachungsgesetzen der meisten Mitgliedstaaten vorgesehen sind; begrüßt insbesondere die Gewährleistung eines uneingeschränkten Zugangs zu wirksamen gerichtlichen Rechtsbehelfen; weist darauf hin, dass der Sonderberichterstatter der Vereinten Nationen für das Recht auf Privatsphäre die mit dem Gesetz zur Regelung von Ermittlungsbefugnissen (Investigatory Powers Act) 2016 eingeführten strengen Garantien in Bezug auf Notwendigkeit, Verhältnismäßigkeit und unabhängige Genehmigung durch eine Justizbehörde begrüßt hat;

15. weist erneut darauf hin, dass der Europäische Gerichtshof für Menschenrechte im September 2018 bestätigt hat, dass die Programme des Vereinigten Königreichs für das Abfangen und die Vorratspeicherung großer Datenmengen, einschließlich „Tempora", unrechtmäßig und mit den für eine demokratische Gesellschaft notwendigen Bedingungen nicht vereinbar sind ([24]);

16. erachtet es für nicht hinnehmbar, dass in den Entwürfen für Angemessenheitsbeschlüsse weder die fehlenden Beschränkungen der Ausübung der Befugnisse des Vereinigten Königreichs in Bezug auf Massendaten noch die tatsächliche Anwendung der gemeinsamen Überwachungsmaßnahmen des Vereinigten Königreichs und der USA, wie sie von Edward Snowden aufgedeckt wurden, berücksichtigt sind, und zwar einschließlich dessen, dass

a) durch das Amt des britischen Datenschutzbeauftragten oder die Gerichte keine wirksame substanzielle Aufsicht über die Inanspruchnahme der Ausnahmeregelung aus Gründen der nationalen Sicherheit im Datenschutzrecht des Vereinigten Königreichs erfolgt;

b) die Beschränkungen der Ausübung der Befugnisse des Vereinigten Königreichs in Bezug auf Massendaten nicht im Gesetz selbst festgelegt sind, wie es der EuGH verlangt (sondern dem Ermessen der Exekutive, das einer „respektvollen" gerichtlichen Kontrolle unterliegt, überlassen werden);

([21]) Angenommene Texte, P9_TA(2020)0033.

([22]) Stellungnahme des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres zu dem Abschluss des Handels- und Kooperationsabkommens im Namen der Union zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits und zu dem Abschluss des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland über die Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen, LIBE_AL(2021)680848.

([23]) Urteil vom 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems, ECLI:EU:C:2020:559.

([24]) Urteil des Europäischen Gerichtshofs für Menschenrechte vom 13. September 2018, Big Brother Watch u. a./Vereinigtes Königreich, Anträge Nr. 58170/13, 62322/14 und 24960/15.

Freitag, 21. Mai 2021

c) die Beschreibung von „Sekundärdaten“ (Metadaten) in den Beschlussentwürfen äußerst irreführend ist und darin außer Acht gelassen wird, dass solche Daten sehr aufschlussreich sein und einen schwerwiegenden Eingriff in die Privatsphäre darstellen können und aufwändigen automatisierten Analysen unterzogen werden (wie der EuGH in der Rechtssache Digital Rights Ireland festgestellt hat ([25])), Metadaten jedoch nach britischem Recht nicht hinreichend vor unberechtigtem Zugriff, Sammelerhebungen und KI-gestützten Analysen durch die britischen Geheimdienste geschützt sind;

d) die „Fünf-Augen“-Agenturen, insbesondere das GCHQ und die Nationale Sicherheitsagentur (NSA), in der Praxis alle nachrichtendienstlichen Daten untereinander austauschen;

weist darauf hin, dass zudem für britische Staatsbürger — gegenüber den USA — einige informelle Sicherheitsgarantien zwischen dem GCHQ und der NSA gelten; äußert sich zutiefst besorgt darüber, dass diese Sicherheitsgarantien Bürger oder Einwohner der EU nicht schützen würden, deren Daten unter Umständen weitergeleitet und an die NSA weitergegeben werden;

17. fordert die Mitgliedstaaten auf, mit dem Vereinigten Königreich Vereinbarungen über den Verzicht auf Spionagetätigkeiten zu schließen, und fordert die Kommission auf, den Austausch mit ihren britischen Amtskollegen zu nutzen, um die Botschaft zu vermitteln, dass der Abschluss von Vereinbarungen über den Verzicht auf Spionagetätigkeiten mit den Mitgliedstaaten die einzige gangbare Option zur Ermöglichung der Angemessenheitsbeschlüsse wäre, wenn an den britischen Überwachungsgesetzen und -praktiken keine Änderungen vorgenommen werden;

Weiterleitung von Daten

18. weist nachdrücklich darauf hin, dass im European Union (Withdrawal) Act 2018 (Gesetz über den Austritt aus der Europäischen Union) vorgesehen ist, dass die bis zum Ende des Übergangszeitraums erfolgte Rechtsprechung des EuGH „beibehaltenes EU-Recht“ wird und somit für das Vereinigte Königreich rechtlich bindend ist; weist darauf hin, dass das Vereinigte Königreich bei der Prüfung der Angemessenheit des Schutzniveaus anderer Drittländer an die in den Urteilen in den Rechtssachen „Schrems I“ und „Schrems II“ des EuGH festgelegten Grundsätze und Bedingungen gebunden ist; ist besorgt darüber, dass die Gerichte des Vereinigten Königreichs die Charta dennoch nicht mehr anwenden werden; weist darauf hin, dass das Vereinigte Königreich nicht mehr in die Zuständigkeit des EuGH fällt, bei dem es sich um die höchste Instanz für die Auslegung der Charta handelt;

19. weist darauf hin, dass die Vorschriften des Vereinigten Königreichs für die Weitergabe personenbezogener Daten nach dem Digital Economy Act 2017 (Gesetz über die digitale Wirtschaft) und für Weiterleitungen von Forschungsdaten den in der DSGVO festgelegten Bestimmungen in der Auslegung durch den EuGH eindeutig nicht „der Sache nach gleichwertig“ sind;

20. ist besorgt darüber, dass sich das Vereinigte Königreich selbst das Recht eingeräumt hat, zu erklären, dass andere Drittländer oder Gebiete einen angemessenen Datenschutz bieten, unabhängig davon, ob das betreffende Drittland oder Gebiet von der EU als Land bzw. Gebiet, das einen derartigen Schutz bietet, angesehen wird; weist erneut darauf hin, dass das Vereinigte Königreich bereits erklärt hat, dass Gibraltar einen solchen Schutz bietet, obwohl die EU dies nicht getan hat; hält es für höchst bedenklich, dass deshalb ein Angemessenheitsbeschluss für das Vereinigte Königreich zur Folge hätte, dass die Unionsvorschriften für die Übermittlung von Daten an Länder oder Gebiete, die nach Unionsrecht nicht als angemessen erachtet werden, umgangen würden;

21. nimmt zur Kenntnis, dass das Vereinigte Königreich am 1. Februar 2021 einen Antrag auf Beitritt zur umfassenden und fortschrittlichen Vereinbarung über eine transpazifische Partnerschaft (Comprehensive and Progressive Agreement for the Trans-Pacific Partnership, CPTPP) übermittelt hat, um insbesondere die Vorteile zeitgemäßer Vorschriften für den digitalen Handel zu nutzen, die einen ungehinderten Datenfluss zwischen den Mitgliedern ermöglichen, unnötige Hindernisse für Unternehmen beseitigen [usw.]; weist mit Sorge darauf hin, dass für acht der elf Unterzeichner der umfassenden und fortschrittlichen Vereinbarung über eine transpazifische Partnerschaft kein Angemessenheitsbeschluss der EU vorliegt; hält mögliche Weiterleitungen personenbezogener Daten von Bürgern und Einwohnern der EU in diese Länder, falls für das Vereinigte Königreich eine positive Angemessenheitsentscheidung getroffen wird, für höchst bedenklich ([26]);

([25]) Urteil des Gerichtshofs vom 8. April 2014, Digital Rights Ireland Ltd gegen Minister for Communications, Marine and Natural Resources u. a. und Kärntner Landesregierung u. a., C-293/12 and C-594/12, ECLI:EU:C:2014:238.

([26]) Pressemitteilung des britischen Ministeriums für internationalen Handel vom 30. Januar 2021 mit dem Titel „UK applies to join huge Pacific free trade area CPTPP“ (Vereinigtes Königreich beantragt Beitritt zu der riesigen Pazifik-Freihandelszone CPTPP).

22. bedauert, dass es die Kommission versäumt hat, die Auswirkungen und potenziellen Risiken des Abkommens zwischen dem Vereinigten Königreich Großbritannien und Nordirland und Japan über eine umfassende und verstärkte Partnerschaft, das Bestimmungen über personenbezogene Daten und das Datenschutzniveau enthält, zu bewerten;

23. ist besorgt darüber, dass das durch die DSGVO gebotene Schutzniveau beeinträchtigt werden würde, sollte das Vereinigte Königreich in künftige Handelsabkommen, darunter Handelsabkommen mit den USA, Bestimmungen zur Übermittlung von Daten aufnehmen;

II. **RICHTLINIE ZUM DATENSCHUTZ BEI DER STRAFVERFOLGUNG**

24. hebt hervor, dass das Vereinigte Königreich das erste Land ist, für das die Kommission den Erlass eines Angemessenheitsbeschlusses gemäß der Richtlinie (EU) 2016/680 empfohlen hat;

25. verweist auf das Abkommen des Vereinigten Königreichs mit den USA über den grenzüberschreitenden Zugang zu Daten ([27]) gemäß dem US-amerikanischen CLOUD Act (Clarifying Overseas Use of Data Act — Gesetz zur Regelung der Verwendung von Daten im Ausland), durch das Übermittlungen für Strafverfolgungszwecke ermöglicht werden; ist zutiefst besorgt, dass US-amerikanische Behörden dadurch einen unzulässigen Zugang zu personenbezogenen Daten von Bürgern und Einwohnern der EU erhalten könnten; teilt die Bedenken des EDSA, dass die im Rahmenabkommen zwischen der EU und den USA ([28]) vorgesehenen Garantien, die sinngemäß angewandt werden, die Kriterien klarer, präziser und zugänglicher Regeln für den Zugang zu personenbezogenen Daten nicht erfüllen oder dass diese Garantien nicht hinreichend verankert sein könnten, um nach britischem Recht wirksam und umsetzbar zu sein;

26. weist erneut darauf hin, dass das Urteil des EuGH in der Rechtssache C-623/17 dahingehend auszulegen ist, dass es einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten des Staates allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln;

27. weist darauf hin, dass der EuGH in dieser Rechtssache geurteilt hat, dass die im Vereinigten Königreich im Rahmen des Regulation of Investigatory Powers Act 2000 (Gesetz zur Regelung von Ermittlungsbefugnissen) durchgeführte Erhebung von Massendaten rechtswidrig war; weist darauf hin, dass diese Regelung seither durch den Investigatory Powers Act (IPA 2016) ersetzt wurde, um die Grundsätze der Notwendigkeit und Verhältnismäßigkeit zu stärken; betont, dass durch den IPA 2016 das Abfangen einer gerichtlichen Überwachung unterliegt und Privatpersonen berechtigt sind, Zugang zu ihren Daten zu erhalten und beim Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse) Beschwerde einzureichen; bedauert jedoch, dass mit dem IPA 2016 die Praxis der Vorratsspeicherung von Massendaten weiterhin ermöglicht wird;

28. ist besorgt über jüngste Berichte, wonach ein Programm für die Erhebung und Vorratsspeicherung von Massendaten Teil eines vom britischen Innenministerium im Rahmen des IPA 2016 geführten Verfahrens ist;

29. weist erneut darauf hin, dass es in seiner Entschließung vom 12. Februar 2020 betont hat, „dass das Vereinigte Königreich keinen direkten Zugang zu den Daten der EU-Informationssysteme haben und sich nicht an den Verwaltungsstrukturen der EU-Agenturen im Raum der Freiheit, der Sicherheit und des Rechts beteiligen kann und dass gleichzeitig der Austausch von Informationen wie personenbezogenen Daten mit dem Vereinigten Königreich strengen Schutzmaßnahmen, Prüf- und Überwachungsbedingungen unterliegen sollte, was auch den gleichwertigen Schutz personenbezogener Daten wie im Unionsrecht einschließt“; nimmt die festgestellten Mängel bei der Umsetzung von Datenschutzrecht durch das Vereinigte Königreich, als es noch Mitglied der EU war, zur Kenntnis; stellt fest,, dass das Vereinigte Königreich eine Kopie des Schengener Informationssystems (SIS) gespeichert und vorgehalten hat; erwartet, dass die Strafverfolgungsbehörden des Vereinigten Königreichs die geltenden Vorschriften beim Austausch personenbezogener Daten künftig uneingeschränkt einhalten werden; weist darauf hin, dass das Vereinigte Königreich nur mehr nach dem Treffer/kein-Treffer-Verfahren Zugriff auf einige Strafverfolgungsdatenbanken der EU hat und rechtlich vom Zugriff auf das SIS ausgeschlossen ist;

([27]) Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America of 3 October 2019 on Access to Electronic Data for the Purpose of Countering Serious Crime (Abkommen zwischen der Regierung des Vereinigten Königreichs Großbritannien und Nordirland und der Regierung der Vereinigten Staaten von Amerika vom 3. Oktober 2019 über den Zugang zu elektronischen Daten für den Zweck der Bekämpfung schwerer Straftaten).

([28]) Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten (ABl. L 336 vom 10.12.2016, S. 3).

30. ist besorgt über die Enthüllung vom Januar 2021, dass 400 000 Strafregistereintragungen versehentlich aus dem nationalen Computer der Polizei des Vereinigten Königreichs gelöscht worden seien; betont, dass dies nicht zum Vertrauen in die Bemühungen des Vereinigten Königreichs im Bereich des Datenschutzes für Strafverfolgungszwecke beiträgt;

31. stellt fest, dass im Entwurf des Angemessenheitsbeschlusses die Rechte jeder Behörde des Vereinigten Königreichs, die nach nationalem Recht befugt ist, personenbezogene Daten aus Gründen der nationalen Sicherheit zu überwachen und zu speichern, gründlich bewertet werden; begrüßt ferner, dass in detaillierten Kontrollberichten über die Behörden, die für die Gemeinschaft der Nachrichtendienste (Intelligence Community) zuständig sind, Informationen über die gegenwärtige Überwachungstätigkeit des Vereinigten Königreichs geliefert werden; fordert die Kommission auf, weiter zu bewerten und zu überwachen, welche Arten von Kommunikationsdaten unter die Befugnisse des Vereinigten Königreichs für die Vorratsspeicherung und das rechtmäßige Abfangen von Daten fallen;

32. weist darauf hin, dass das Handels- und Kooperationsabkommen zwischen der Europäischen Union und dem Vereinigten Königreich Titel zum Austausch von DNA-, Fingerabdruck- und Fahrzeugregisterdaten, zur Übermittlung und Verarbeitung von Fluggastdatensätzen (PNR), zur Zusammenarbeit bei operativen Informationen und zur Zusammenarbeit mit Europol und Eurojust umfasst, die unabhängig von der Angemessenheitsentscheidung gelten werden; weist jedoch erneut darauf hin, dass in der Stellungnahme des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres vom Februar 2021 zu diesem Handels- und Kooperationsabkommen Bedenken geäußert wurden, was die spezielle Verwendung und längere Vorratsspeicherung von personenbezogenen Daten anbelangt, die dem Vereinigten Königreich nach den Prüm- und PNR-Titeln des Handels- und Kooperationsabkommens zugestanden werden und die nicht im Einklang mit den Verwendungszwecken und Vorratsspeicherfristen in den Mitgliedstaaten stehen; weist erneut auf das Recht hin, vor dem EuGH Klage zu erheben, um die Rechtmäßigkeit des vorgeschlagenen internationalen Abkommens und insbesondere dessen Vereinbarkeit mit dem Schutz eines Grundrechts zu überprüfen ([29]);

Fazit

33. fordert die Kommission auf, den Unternehmen in der EU zuzusichern, dass der Angemessenheitsbeschluss eine solide, ausreichende und zukunftsorientierte Rechtsgrundlage für Datenübermittlungen bieten wird; erachtet es als sehr wichtig, dass sichergestellt wird, dass dieser Angemessenheitsbeschluss einer möglichen Prüfung durch den EuGH standhält, und betont, dass deshalb alle in der Stellungnahme des EDSA formulierten Empfehlungen übernommen werden sollten;

34. begrüßt, dass die Angemessenheitsbeschlüsse nur vier Jahre lang gelten werden, da das Vereinigte Königreich beschließen könnte, die Rechtsvorschriften, die Gegenstand der Angemessenheitsbewertung der Kommission waren, nun, da es kein EU-Mitgliedstaat mehr ist, zu ändern; fordert die Kommission auf, in der Zwischenzeit das Datenschutzniveau im Vereinigten Königreich in Recht und Praxis weiter zu überwachen und vor der Verlängerung des Angemessenheitsbeschlusses im Jahr 2025 eine gründliche Bewertung vorzunehmen;

35. vertritt die Auffassung, dass die Kommission durch die Annahme der beiden Durchführungsbeschlüsse, die nicht mit dem EU-Recht vereinbar sind, ohne auf alle in dieser Entschließung geäußerten Bedenken eingegangen zu sein, über die durch die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 übertragenen Durchführungsbefugnisse hinausgeht; lehnt deshalb die beiden Durchführungsrechtsakte ab, weil die Entwürfe von Durchführungsbeschlüssen nicht mit dem EU-Recht vereinbar sind;

36. fordert die Kommission auf, die beiden Entwürfe von Durchführungsbeschlüssen zu ändern, um sie in jeder Hinsicht mit dem EU-Recht und der Rechtsprechung in Einklang zu bringen;

37. fordert die nationalen Datenschutzbehörden auf, die Übermittlung personenbezogener Daten auszusetzen, auf die die Geheimdienste des Vereinigten Königreichs wahllos zugreifen könnten, wenn die Kommission ihre Angemessenheitsbeschlüsse in Bezug auf das Vereinigte Königreich annimmt, bevor das Vereinigte Königreich die vorstehend genannten Probleme gelöst hat;

38. fordert die Kommission und die zuständigen Behörden des Vereinigten Königreichs auf, einen Aktionsplan zu erstellen, um so bald wie möglich die in den Stellungnahmen des EDSA festgestellten Mängel zu beheben und andere offene Fragen im Bereich des Datenschutzes des Vereinigten Königreichs zu klären, was eine Voraussetzung für den endgültigen Angemessenheitsbeschluss sein muss;

39. fordert die Kommission auf, das Datenschutzniveau sowie die Rechtsvorschriften und die Massenüberwachung im Vereinigten Königreich in Recht und Praxis weiter genau zu überwachen; weist darauf hin, dass es in Kapitel V der DSGVO andere rechtliche Möglichkeiten für die Übermittlung personenbezogener Daten an das Vereinigte Königreich gibt; weist erneut darauf hin, dass Leitlinien des EDSA, die sich auf Ausnahmen für bestimmte Fälle im Sinne von Artikel 49 DSGVO stützen, die Ausnahme sein müssen;

([29]) Entschließung des Europäischen Parlaments zu dem Entwurf einer Entscheidung der Kommission über die Angemessenheit des Schutzes personenbezogener Daten, die in den Fluggastdatensätzen (PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden (ABl. C 103 E vom 29.4.2004, S. 665).

40. bedauert, dass die Kommission die Forderungen des Parlaments ignoriert hat, den Datenschutzschild auszusetzen, bis die US-Behörden seine Bestimmungen einhalten, sondern es stattdessen stets vorgezogen hat, „die Lage zu beobachten", ohne konkrete Ergebnisse in Bezug auf den Datenschutz für Einzelpersonen und die Rechtssicherheit für Unternehmen zu erzielen; fordert die Kommission nachdrücklich auf, aus ihren bisherigen Versäumnissen, Forderungen des Parlaments und von Sachverständigen in Bezug auf den Abschluss und die Überwachung früherer Angemessenheitsbeschlüsse zu beachten, zu lernen und die ordnungsgemäße Durchsetzung des EU-Datenschutzrechts nicht nach Beschwerden einzelner Bürger dem Gerichtshof der Europäischen Union zu überlassen;

41. fordert die Kommission auf, Recht und Praxis des Datenschutzes im Vereinigten Königreich engmaschig zu überwachen und das Parlament bei etwaigen künftigen Änderungen in den Datenschutzregelungen des Vereinigten Königreichs unverzüglich zu informieren und zu konsultieren und dem Parlament im Zuge des neuen institutionellen Rahmens eine Kontrollfunktion einzuräumen, die auch die einschlägigen Gremien wie etwa den Sonderausschuss für Zusammenarbeit im Bereich der Strafverfolgung und Justiz erfasst;

o

o o

42. beauftragt seinen Präsidenten, diese Entschließung der Kommission, den Mitgliedstaaten und der Regierung des Vereinigten Königreichs zu übermitteln.