Europäisches Parlament
2019-2024

ANGENOMMENE TEXTE

P9_TA(2023)0204

Angemessenheit des vom Datenschutzrahmen EU-USA gebotenen Schutzes

Entschließung des Europäischen Parlaments vom 11. Mai 2023 zur Angemessenheit des vom Datenschutzrahmen zwischen der EU und den USA gebotenen Schutzes (2023/2501(RSP))

Das Europäische Parlament,

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“), insbesondere auf die Artikel 7, 8, 16, 47 und 52,

– unter Hinweis auf das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximilian Schrems gegen Data Protection Commissioner („Schrems I“)[1],

– unter Hinweis auf das Urteil des EuGH vom 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems („Schrems II“)[2],

– unter Hinweis auf seine Untersuchung zu den Enthüllungen von Edward Snowden über die elektronische Massenüberwachung von EU-Bürgern, einschließlich der Feststellungen in seiner Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres[3],

– unter Hinweis auf seine Entschließung vom 26. Mai 2016 zur transatlantischen Datenübermittlung[4],

– unter Hinweis auf seine Entschließung vom 6. April 2017 zur Angemessenheit des vom

---

1 Urteil vom 6. Oktober 2015, Maximilian Schrems gegen Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.
2 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.
3 ABl. C 378 vom 9.11.2017, S. 104.
4 ABl. C 76 vom 28.2.2018, S. 82.

EU-US-Datenschutzschild gebotenen Schutzes[1],

– unter Hinweis auf seine Entschließung vom 5. Juli 2018 zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes[2],

– unter Hinweis auf seine Entschließung vom 20. Mai 2021 zum Urteil des EuGH vom 16. Juli 2020 – Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems („Schrems II“), Rechtssache C-311/18[3],

– unter Hinweis auf den Entwurf eines Durchführungsbeschlusses der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über das angemessene Schutzniveau für personenbezogene Daten im Rahmen des Datenschutzrahmens zwischen der EU und den USA,

– unter Hinweis auf die Executive Order 14086 des Präsidenten der Vereinigten Staaten vom 7. Oktober 2022 zur Verbesserung der Sicherheitsvorkehrungen für nachrichtendienstliche Tätigkeiten der Vereinigten Staaten im Bereich Fernmelde- und elektronische Aufklärung (Enhancing Safeguards For United States Signals Intelligence Activities),

– unter Hinweis auf die Executive Order 12333 des Präsidenten der Vereinigten Staaten vom 4. Dezember 1981 über nachrichtendienstliche Tätigkeiten der Vereinigten Staaten,

– unter Hinweis auf die vom US-Generalstaatsanwalt erlassene Verordnung über ein Datenschutz-Überprüfungsgericht („Data Protection Review Court“) (im Folgenden „Verordnung des US-Generalstaatsanwalts“),

– 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, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[4], insbesondere auf Kapitel V,

– 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[5],

– unter Hinweis auf die Referenzgrundlage für Angemessenheit der Artikel-29-Datenschutzgruppe (WP 254/rev.01), die vom Europäischen Datenschutzausschuss (EDSA) bestätigt wurde, sowie auf die Empfehlung 01/2020 des EDSA zu Maßnahmen, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des Datenschutzniveaus der EU zu gewährleisten, und die Empfehlung 02/2020 des EDSA zu den wesentlichen europäischen Garantien für Überwachungsmaßnahmen,

– unter Hinweis auf die Stellungnahme 5/2023 des Europäischen Datenschutzausschusses vom 28. Februar 2023 zu dem Entwurf eines Durchführungsbeschlusses der Kommission über die Angemessenheit des Schutzes personenbezogener Daten im

---

1 ABl. C 298 vom 23.8.2018, S. 73.
2 ABl. C 118 vom 8.4.2020, S. 133.
3 ABl. C 15 vom 12.1.2022, S. 176.
4 ABl. L 119 vom 4.5.2016, S. 1.
5 ABl. L 201 vom 31.7.2002, S. 37.

Rahmen des EU-US-Datenschutzrahmens,

– gestützt auf Artikel 132 Absatz 2 seiner Geschäftsordnung,

A. in der Erwägung, dass der EuGH mit dem Urteil „Schrems I“ die auf die Richtlinie 95/46/EG gestützte Entscheidung der Kommission vom 26. Juli 2000 über die Angemessenheit des durch die Safe-Harbour-Grundsätze gewährleisteten Schutzes und der dazu vom Handelsministerium der USA veröffentlichten „Häufig gestellten Fragen“ (FAQ) [1] für ungültig erklärte und darauf hinwies, dass der wahllose Zugriff von Nachrichtendiensten auf den Inhalt von elektronischer Kommunikation den Wesensgehalt des in Artikel 7 der Charta verankerten Grundrechts auf Vertraulichkeit der Kommunikation verletzt; in der Erwägung, dass der Gerichtshof darauf hinwies, dass ein Drittland für die Zwecke eines Angemessenheitsbeschlusses nicht ein identisches, sondern ein dem in der Rechtsordnung der Union garantierten Niveau „der Sache nach gleichwertiges“ Schutzniveau gewährleisten muss, was auf unterschiedliche Weise sichergestellt werden kann;

B. in der Erwägung, dass der EuGH im Urteil „Schrems II“ den auf die Richtlinie 95/46/EG gestützten Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes[2] für ungültig erklärte und feststellte, dass dieser mit Blick auf eine Massenüberwachung keine hinreichenden Rechtsbehelfe für Personen vorsieht, die keine amerikanischen Staatsbürger sind, und dass dadurch der Wesensgehalt des in Artikel 47 der Charta verankerten Rechts auf einen wirksamen Rechtsbehelf verletzt wird;

C. in der Erwägung, dass der Präsident der Vereinigten Staaten von Amerika am 7. Oktober 2022 die Executive Order 14086 zur Verbesserung der Sicherheitsvorkehrungen für nachrichtendienstliche Tätigkeiten der Vereinigten Staaten im Bereich Fernmelde- und elektronische Aufklärung (Enhancing Safeguards For United States Signals Intelligence Activities) unterzeichnete (EO 14086);

D. in der Erwägung, dass die Kommission am 13. Dezember 2022 das Verfahren zur Annahme eines Angemessenheitsbeschlusses für den Datenschutzrahmen zwischen der EU und den USA eingeleitet hat;

E. in der Erwägung, dass die Kommission bei der Prüfung des von einem Drittland gewährten Schutzniveaus verpflichtet ist, den Inhalt der in diesem Land geltenden Vorschriften, die sich aus seinem innerstaatlichen Recht oder seinen internationalen Verpflichtungen ergeben, sowie die praktische Umsetzung zu bewerten, mit der die Einhaltung dieser Vorschriften sichergestellt werden soll; in der Erwägung, dass die Kommission für den Fall, dass eine solche Bewertung in Bezug auf die Angemessenheit und Gleichwertigkeit nicht zufriedenstellend ausfällt, davon absehen sollte, einen Angemessenheitsbeschluss zu fassen, da dies von der Umsetzung einschlägiger Garantien abhängig ist; in der Erwägung, dass die Kommission verpflichtet ist, die Anerkennung der Angemessenheit auszusetzen, wenn keine Gleichwertigkeit mehr besteht; in der Erwägung, dass die Datenschutz-Grundverordnung (DSGVO) vorschreibt, dass die einschlägige Bewertung ein kontinuierlicher Prozess sein sollte,

---

1 ABl. L 215 vom 25.8.2000, S. 7.

2 ABl. L 207 vom 1.8.2016, S. 1.

bei dem Änderungen der geltenden Vorschriften und Verfahren berücksichtigt werden;

F. in der Erwägung, dass die Möglichkeit, personenbezogene Daten über Grenzen hinweg zu übertragen, eine Triebfeder für Innovation, Produktivität und wirtschaftliche Wettbewerbsfähigkeit sein kann, solange angemessene Garantien vorgesehen sind; in der Erwägung, dass bei solchen Datenübertragungen das Recht auf den Schutz personenbezogener Daten und das Recht auf Privatsphäre uneingeschränkt gewahrt werden sollten; in der Erwägung, dass der in der Charta verankerte Schutz der Grundrechte eines der Ziele der EU darstellt;

G. in der Erwägung, dass die DSGVO auf alle Unternehmen anwendbar ist, die personenbezogene Daten von betroffenen Personen in der EU verarbeiten, wenn diese Verarbeitungstätigkeiten im Zusammenhang damit stehen, dass diesen Personen in der Union Waren oder Dienstleistungen angeboten werden oder ihr Verhalten, sofern es in der Union erfolgt, beobachtet wird;

H. in der Erwägung, dass eine Massenüberwachung, d. h. die willkürliche Erhebung von Daten ohne jegliche Garantie zur Begrenzung des Eingriffs in die Privatsphäre des Einzelnen, durch staatliche Akteure das Vertrauen der europäischen Bürger und Unternehmen in digitale Dienste und damit in die digitale Wirtschaft untergräbt; in der Erwägung, dass es US-Behörden zwar untersagt ist, Massendaten von US-Bürgern, die in den Vereinigten Staaten leben, zu erheben, dieses Verbot jedoch nicht für EU-Bürger gilt; in der Erwägung, dass eine Massenüberwachung durch staatliche Akteure illegal ist und dem Vertrauen der EU-Bürger und der Unternehmen in digitale Dienste und somit in die digitale Wirtschaft zuwiderläuft;

I. in der Erwägung, dass es stets Aufgabe der für die Verarbeitung Verantwortlichen sein sollte, dafür Sorge zu tragen, dass die Datenschutzvorschriften eingehalten werden, und dies bei jeder Verarbeitung von Daten nachzuweisen, gleich um welche Art der Verarbeitung es sich handelt, in welchem Umfang und Rahmen sie erfolgt, welchem Zweck sie dient und welche Risiken sie für die betroffenen Personen birgt;

J. in der Erwägung, dass es in den Vereinigten Staaten auf Bundesebene keine Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz gibt; in der Erwägung, dass in der Executive Order 14086 wichtige Datenschutzkonzepte wie die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit definiert werden, was im Vergleich zu früheren Übertragungsmechanismen einen bedeutenden Fortschritt darstellt; in der Erwägung, dass genau überwacht werden muss, wie diese Grundsätze ausgelegt werden; in der Erwägung, dass es aufgrund der mangelnden Transparenz der Verfahren vor dem Datenschutz-Überprüfungsgericht möglicherweise nicht möglich ist, umfassend zu bewerten, wie diese Grundsätze in die Rechtsordnung der Vereinigten Staaten umgesetzt werden;

1. weist erneut darauf hin, dass die Achtung des Privat- und Familienlebens und der Schutz personenbezogener Daten rechtlich durchsetzbare Grundrechte sind, die in den Verträgen, der Charta und der Europäischen Menschenrechtskonvention sowie in Gesetzen und in der Rechtsprechung verankert sind; betont, dass Angemessenheitsbeschlüsse im Rahmen der DSGVO keine politischen, sondern rechtliche Entscheidungen sind, und dass das Recht auf Privatsphäre und das Recht auf Datenschutz nicht gegen kommerzielle oder politische Interessen aufgewogen werden dürfen sondern nur gegen andere Grundrechte;

2. nimmt zur Kenntnis, dass mit der Executive Order 14086 Anstrengungen unternommen wurden, um den nachrichtendienstlichen Tätigkeiten der USA im Bereich Fernmelde- und elektronische Aufklärung Grenzen zu setzen, indem dafür gesorgt wurde, dass die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit auf den US-Rechtsrahmen für Fernmelde- und elektronische Aufklärung Anwendung finden und eine Liste legitimer Ziele für solche Tätigkeiten bereitgestellt wird; stellt fest, dass diese Grundsätze für alle US-Nachrichtendienste verbindlich sein dürften und von Betroffenen im Rahmen des in der Executive Order 14086 vorgesehenen Verfahrens geltend gemacht werden können; betont, dass die Executive Order 14086 erhebliche Verbesserungen enthält, mit denen sichergestellt werden soll, dass diese Grundsätze dem EU-Recht im Wesentlichen gleichwertig sind; weist jedoch darauf hin, dass es sich bei diesen Grundsätzen um seit Langem bestehende zentrale Elemente des EU-Datenschutzrechts handelt und dass ihre inhaltliche Definition in der Executive Order 14086 nicht mit ihrer Definition im EU-Recht und ihrer Auslegung durch den EuGH übereinstimmt; weist außerdem darauf hin, dass diese Grundsätze für die Zwecke des Datenschutzrahmens zwischen der EU und den USA ausschließlich im Lichte des Rechts und der Rechtstraditionen der USA und nicht denen der EU ausgelegt würden; stellt fest, dass die Executive Order 12 legitime Ziele auflistet, die mit der Sammlung von Daten durch die Fernmelde- und elektronische Aufklärung verfolgt werden dürfen, und fünf Ziele, bei denen die Sammlung von Daten durch die Fernmelde- und elektronische Aufklärung untersagt ist; stellt fest, dass die Liste der legitimen nationalen Sicherheitsziele durch den Präsidenten der USA erweitert und geändert werden kann, wobei es keinerlei Verpflichtung gibt, die entsprechenden Aktualisierungen zu veröffentlichen oder die EU davon in Kenntnis zu setzen; weist darauf hin, dass gemäß der Executive Order 14086 die Fernmelde- und elektronische Aufklärung auf eine Weise erfolgen muss, die mit Blick auf die „validierte nachrichtendienstliche Priorität“ erforderlich und verhältnismäßig ist, was auf eine breite Auslegung dieser Begriffe hinzudeuten scheint; betont, dass für eine umfassende Bewertung der Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit im Zusammenhang mit der Executive Order 14086 diese Grundsätze zur Anwendung gebracht und in den Strategien und Verfahren der US-Geheimdienste umgesetzt werden müssten; bringt jedoch seine Sorge darüber zum Ausdruck, dass die Analysten nicht für jede Überwachungsentscheidung eine Bewertung der Verhältnismäßigkeit vornehmen müssen;

3. stellt fest, dass die Executive Order 14086 die massenhafte Erhebung von Daten, einschließlich des Inhalts von Mitteilungen, durch Fernmelde- und elektronische Aufklärung gestattet; weist zugleich darauf hin, dass gemäß der Executive Order 14086 die gezielte Erhebung von Daten der Massenerhebung vorgezogen werden soll; stellt fest, dass die Executive Order 14086 zwar mehrere Schutzklauseln für den Fall der Massenerhebung enthält, aber keine unabhängige vorherige Einwilligung in die Massenerhebung vorsieht, und dass eine solche Einwilligung auch in der Executive Order 12333 nicht vorgesehen ist; erinnert daran, dass der EuGH in der Rechtssache „Schrems II“ festgestellt hat, dass die Überwachung durch die USA nicht dem EU-Recht entsprach, weil kein „objektives Kriterium“ verlangt wurde, das den Eingriff der Regierung in die Privatsphäre „rechtfertigen“ könnte; weist darauf hin, dass dadurch der Zweck der Ziele als Schutzmaßnahme zur Begrenzung der Aktivitäten der US-Geheimdienste untergraben wird; erinnert daran, dass das „Privacy and Civil Liberties Oversight Board“ nach der Presidential Policy Directive 28 (PPD 28), die die Grundlage für den Beschluss zur Angemessenheit des Datenschutzschilds bildete, einen

Überprüfungsbericht[1] herausgegeben hat und zu dem Schluss gekommen ist, dass mit der PPD-28 im Wesentlichen die bereits bestehenden Praktiken der Nachrichtendienste festgeschrieben wurden; ist überzeugt, dass mit der PPD-28 die elektronische Massenüberwachung von EU-Bürgern durch US-Behörden nicht aufhören wird;

4. teilt die Bedenken des EDSA in Bezug auf die Executive Order 14086, wonach diese keine hinreichenden Garantien für den Fall der Massenerhebung von Daten biete, und zwar insbesondere in Bezug auf das Fehlen einer unabhängigen vorherigen Einwilligung, klarer und strenger Vorschriften für die Datenspeicherung und die vorübergehende Massenerhebung sowie das Fehlen strengerer Garantien für die Weitergabe von durch Massenerhebung gewonnenen Daten; weist insbesondere auf die besondere Besorgnis hin, dass Strafverfolgungsbehörden – sollte die Weitergabe an US-Behörden keinen weiteren Beschränkungen unterliegen – Zugang zu Daten erhalten würden, auf die ihnen andernfalls der Zugriff untersagt wäre; weist darauf hin, dass durch die Weitergabe die Risiken für den Datenschutz effektiv vervielfacht werden; stellt fest, dass der EDSA die Aufnahme einer rechtsverbindlichen Verpflichtung gefordert hat, zu analysieren und festzustellen, ob ein Drittland ein akzeptables Mindestmaß an Garantien bietet;

5. weist darauf hin, dass die Executive Order 14086 nicht auf Daten anwendbar ist, auf die die Behörden auf anderem Wege zugreifen, beispielsweise im Rahmen des Cloud Act oder des Patriot Act der Vereinigten Staaten, im Wege kommerzieller Datenkäufe oder über freiwillige Vereinbarungen zur gemeinsamen Nutzung von Daten;

6. weist darauf hin, dass das eigentliche Problem die Überwachung von Nicht-US-Personen nach US-Recht ist und dass europäische Bürger diesbezüglich keinen wirksamen gerichtlichen Rechtsbehelf einlegen können; fordert, dass EU-Bürgern die gleichen Rechte und Privilegien wie US-Bürgern eingeräumt werden sollten, wenn es um die Aktivitäten der US-Geheimdienste und den Zugang zu US-Gerichten geht;

7. stellt fest, dass der Begriff „signals intelligence“ (Fernmelde- und elektronische Aufklärung) gemäß der US-amerikanischen Auslegung alle im Foreign Intelligence Surveillance Act (FISA) vorgesehenen Arten des Datenzugriffs umfasst, einschließlich des Zugriffs von Anbietern von Fernverarbeitungsdiensten, die mit dem FISA Amendment Act S1881a im Jahr 2008 hinzugefügt wurden; fordert die Kommission auf, bei künftigen Verhandlungen die Definition und den Umfang des Begriffs „signals intelligence“ in der Executive Order 14086 zu klären; erinnert daran, dass die US-Regierung gemäß Abschnitt 702 des FISA nach wie vor die Befugnis für sich in Anspruch nimmt, jede nichtamerikanische Person im Ausland ins Visier zu nehmen, um ausländische nachrichtendienstliche Erkenntnisse im weitesten Sinne zu erlangen;

8. weist darauf hin, dass ein neuer Rechtsbehelfsmechanismus geschaffen wurde, der es betroffenen Personen in der EU ermöglicht, eine Beschwerde einzureichen; betont gleichzeitig, dass die Entscheidungen des Datenschutz-Überprüfungsgerichts als Verschlusssache eingestuft und weder veröffentlicht noch dem Beschwerdeführer zugänglich gemacht werden, der lediglich darüber informiert wird, dass bei der Überprüfung keine erfassten Verstöße festgestellt wurden oder das Datenschutz-Überprüfungsgericht geeignete Maßnahmen angeordnet hat, wodurch das Recht der

---

[1] PCLOB, Report to the President on the Implementation of Presidential Directive 28: Signals Intelligence Activities.

betroffenen Personen auf Zugang zu ihren Daten oder auf Berichtigung ihrer Daten unterlaufen wird; stellt mit Sorge fest, dass dies bedeutet, dass eine Person, die ein Verfahren anstrengt, keine Chance hätte, über den inhaltlichen Ausgang des Verfahrens informiert zu werden, und dass die Entscheidung endgültig wäre; stellt fest, dass das vorgeschlagene Rechtsbehelfsverfahren kein Rechtsmittel vor einem Bundesgericht vorsieht und daher unter anderem dem Beschwerdeführer keine Möglichkeit bietet, Schadenersatz zu fordern; fordert die Kommission auf, die Verhandlungen mit den Vereinigten Staaten fortzusetzen, um die notwendigen Änderungen zu erreichen und diesen Bedenken Rechnung zu tragen;

9. ist der Auffassung, dass die Executive Order 14086 mehrere Garantien zur Sicherstellung der Unabhängigkeit der Richter des Gerichts zur Datenschutzüberprüfung vorsieht, was auch vom EDSA in seiner Stellungnahme anerkannt wird; weist darauf hin, dass das Datenschutz-Überprüfungsgericht Teil der Exekutive und nicht der Judikative ist und dass seine Richter für eine feste Amtszeit von vier Jahren ernannt werden; hebt ferner hervor, dass der amerikanische Präsident die Entscheidungen des Datenschutz-Überprüfungsgerichts außer Kraft setzen kann, sogar im Geheimen; weist darauf hin, dass es gemäß dem neuen Rechtsbehelfsmechanismus dem US-Generalstaatsanwalt zwar nicht gestattet ist, die Richter des Datenschutz-Überprüfungsgerichts zu entlassen oder zu beaufsichtigen, die entsprechenden Befugnisse des amerikanischen Präsidenten davon aber unberührt bleiben; betont, dass die Unabhängigkeit dieser Richter nicht gewährleistet ist, solange der amerikanische Präsident Richter des Datenschutz-Überprüfungsgerichts während ihrer Amtszeit abberufen kann; weist darauf hin, dass die Kommission im Falle der Annahme des Beschlusses die Anwendung der Garantien genau überwachen müsste, um die Unabhängigkeit in der Praxis sicherzustellen; weist darauf hin, dass ein Beschwerdeführer von einem vom Datenschutz-Überprüfungsgericht benannten „Sonderanwalt“ vertreten würde, für den keine Anforderungen im Hinblick auf Unabhängigkeit gelten; fordert die Kommission auf, dafür zu sorgen, dass für den Fall, dass ein Angemessenheitsbeschluss angenommen wird, das Erfordernis der Unabhängigkeit darin aufgenommen wird; kommt nach derzeitiger Lage zu dem Schluss, dass das Datenschutz-Überprüfungsgericht die in Artikel 47 der Charta festgelegten Anforderungen an die Unabhängigkeit und Unparteilichkeit nicht erfüllt; stellt fest, dass der Privacy and Civil Liberties Oversight Board zwar die Funktionsweise des neuen Rechtsbehelfsverfahrens unabhängig überprüfen würde, der Umfang einer solchen Überprüfung jedoch begrenzt wäre;

10. stellt fest, dass die Vereinigten Staaten zwar einen neuen Rechtsbehelfsmechanismus für Angelegenheiten im Zusammenhang mit dem Zugang von Behörden zu Daten vorgesehen haben, dass aber noch Fragen zur Wirksamkeit der im Zusammenhang mit gewerblichen Angelegenheiten verfügbaren Rechtsbehelfe offen sind, für die sich im Angemessenheitsbeschluss nichts geändert hat; stellt fest, dass die Mechansimen, die auf die Beilegung solcher Angelegenheiten abzielen, weitgehend dem Ermessen der Unternehmen überlassen bleiben, die alternative Abhilfemaßnahmen wie Streitbeilegungsmechanismen oder die Heranziehung unternehmensinterner Datenschutzprogramme wählen können; fordert die Kommission auf, im Falle der Annahme eines Angemessenheitsbeschlusses die Wirksamkeit dieser Rechtsbehelfsmachanismen genau zu überwachen;

11. stellt fest, dass die europäischen Unternehmen Rechtssicherheit brauchen und verdienen; betont, dass die aufeinanderfolgenden Datenübertragungsmechanismen, die

im Nachhinein vom EuGH wieder aufgehoben wurden, den europäischen Unternehmen zusätzliche Kosten verursacht haben; erkennt daher die Notwendigkeit an, für Rechtssicherheit zu sorgen und Situationen zu vermeiden, in denen sich Unternehmen ständig auf neue rechtliche Rahmenbedingungen einstellen müssen, was für Kleinst-, Klein- und mittlere Unternehmen eine besondere Belastung darstellen könnte; ist besorgt, dass der Angemessenheitsbeschluss, sollte er angenommen werden, (wie seine Vorgänger) vom EuGH für ungültig erklärt werden könnte, was zu einer anhaltenden Rechtsunsicherheit, weiteren Kosten und Störungen für die europäischen Bürger und Unternehmen führen würde;

12. weist darauf hin, dass die Vereinigten Staaten im Gegensatz zu allen anderen Drittländern, für die im Rahmen der DSGVO ein Angemessenheitsbeschluss angenommen wurde, über kein Datenschutzgesetz auf Bundesebene verfügen; weist darauf hin, dass die Executive Order 14086 in ihrer Anwendung nicht klar, präzise und vorhersehbar ist, da sie vom amerikanischen Präsidenten, der zudem befugt ist, geheime Executive Orders zu erlassen, jederzeit geändert oder aufgehoben werden kann; nimmt zur Kenntnis, dass die Überprüfung der Feststellung der Angemessenheit ein Jahr nach dem Zeitpunkt der Mitteilung des Angemessenheitsbeschlusses an die Mitgliedstaaten und anschließend mindestens alle vier Jahre durchgeführt würde; fordert die Kommission für den Fall, dass ein künftiger Angemessenheitsbeschluss angenommen wird, auf, gemäß der Stellungnahme des EDSA mindestens alle drei Jahre nachträgliche Überprüfungen durchzuführen; ist besorgt darüber, dass keine Verfallsklausel vorgesehen ist, derzufolge der Beschluss vier Jahre nach Inkrafttreten automatisch seine Gültigkeit verlieren würde und die Kommission anschließend eine neue Beurteilung vornehmen müsste; ist besorgt darüber, dass im Fehlen einer Verfallsklausel in diesem Angemessenheitsbeschluss eine nachsichtigere Haltung gegenüber den Vereinigten Staaten zum Ausdruck kommt, und das obwohl der US-Datenschutzrahmen auf einer Executive Order beruht, die geheime Änderungen zulässt und ohne Zustimmung des Kongresses und ohne Unterrichtung der EU-Partner geändert werden kann; fordert die Kommission daher auf, eine solche Klausel in den Beschluss aufzunehmen;

13. teilt die Bedenken des EDSA in Bezug auf die Rechte betroffener Personen, das Fehlen wichtiger Definitionen und spezieller Vorschriften für automatisierte Entscheidungsprozesse und Profiling, die mangelnde Klarheit über die Anwendung der Grundsätze des Datenschutzrahmens auf Auftragsverarbeiter und die Notwendigkeit, Weiterübertragungen von Daten, durch die das Schutzniveau untergraben wird, zu verhindern;

14. betont, dass Angemessenheitsbeschlüsse klare und strenge Überwachungs- und Überprüfungsmechanismen enthalten müssen, damit sichergestellt ist, dass die Beschlüsse zukunftssicher sind oder je nach Bedarf aufgehoben oder geändert werden können und das Grundrecht der EU-Bürger auf Datenschutz jederzeit gewährleistet ist; betont, dass jeder künftige Angemessenheitsbeschluss einer kontinuierlichen Überprüfung unterzogen werden sollte, bei der den rechtlichen und praktischen Entwicklungen in den Vereinigten Staaten Rechnung zu tragen ist;

Schlussfolgerungen

15. erinnert daran, dass das Parlament die Kommission in seiner Entschließung vom 20. Mai 2021 aufgefordert hat, keinen neuen Angemessenheitsbeschluss in Bezug auf die Vereinigten Staaten zu erlassen, sofern keine bedeutsamen Reformen, insbesondere

für Zwecke der nationalen Sicherheit und der Nachrichtendienste, in die Wege geleitet werden; betrachtet die Executive Order14086 nicht als hinreichend bedeutsam; weist erneut darauf hin, dass die Kommission die Aufgabe des Schutzes der Grundrechte der EU-Bürger nicht dem nicht dem Gerichtshof der Europäischen Union überlassen sollte, der sich mit Klagen einzelner Bürger befasst;

16. weist darauf hin, dass die Kommission die Angemessenheit in Bezug auf ein Drittland auf der Grundlage der geltenden Rechtsvorschriften und Praktiken im Lichte der Rechtssachen Schrems I und Schrems II und der Datenschutz-Grundverordnung (Erwägungsgrund 104) nicht nur inhaltlich, sondern auch im Hinblick auf ihre prakitsche Umsetzung bewerten muss;

17. stellt fest, dass die Änderungen an den vom US-Handelsministerium herausgegebenen Grundsätzen für den Datenschutzrahmen im Vergleich zu den Grundsätzen des Datenschutzschilds nicht ausreichen, um ein im Wesentlichen der DSGVO gleichwertiges Schutzniveau zu bieten;

18. stellt fest, dass die Vereinigten Staaten zwar bedeutende Zusagen machen, um den Zugang zu Rechtsbehelfen und die Vorschriften über die Datenverarbeitung durch Behörden zu verbessern, dass die US-Geheimdienste jedoch bis Oktober 2023 Zeit haben, ihre Methoden und Praktiken im Einklang mit den Verpflichtungen der Executive Order 14086 zu ändern und dass der US-Generalstaatsanwalt die EU und ihre Mitgliedstaaten noch nicht als Länder benannt hat, die befugt sind, vor dem Datenschutz-Überprüfungsgericht einen Rechtsbehelf einzulegen; betont, dass das bedeutet, dass die Kommission nicht in der Lage war, die Wirksamkeit der vorgeschlagenen Rechtsbehelfe und sonstigen Maßnahmen in Bezug auf den Zugang zu Daten „in der Praxis“ zu bewerten; kommt daher zu dem Schluss, dass die Kommission erst dann mit dem nächsten Schritt eines Angemessenheitsbeschlusses fortfahren kann, wenn diese Fristen und Zielvorgaben von den Vereinigten Staaten erfüllt worden sind, damit sichergestellt ist, dass die Zusagen in der Praxis eingehalten wurden;

19. kommt zu dem Schluss, dass mit dem Datenschutzrahmen zwischen der EU und den USA keine wesentliche Gleichwertigkeit im Hinblick auf das Schutzniveau geschaffen wird; fordert die Kommission auf, die Verhandlungen mit ihren US-amerikanischen Partnern fortzusetzen, um einen Mechanismus zu schaffen, der eine solche Gleichwertigkeit gewährleistet und das nach dem Datenschutzrecht der Union und der Charta in der Auslegung durch den EuGH erforderliche angemessene Schutzniveau bietet; fordert die Kommission auf, den Angemessenheitsbeschluss erst anzunehmen, wenn alle in dieser Entschließung und in der Stellungnahme des EDSA enthaltenen Empfehlungen vollständig umgesetzt sind;

20. fordert die Kommission auf, im Interesse der Unternehmen und Bürger in der EU zu handeln und sicherzustellen, dass der vorgeschlagene Rahmen eine solide, ausreichende und zukunftsorientierte Rechtsgrundlage für Datenübermittlungen zwischen der EU und den USA bietet; erwartet, dass jeder Angemessenheitsbeschluss, sollte er angenommen werden, erneut vor dem EuGH angefochten wird; hebt hervor, dass die Kommission – sollte der Angemessenheitsbeschluss vom EuGH erneut für ungültig erklärt werden – die Verantwortung dafür trägt, dass die Rechte der EU-Bürger nicht geschützt werden;

°

° °

21. beauftragt seine Präsidentin, diese Entschließung dem Rat und der Kommission sowie dem Präsidenten und dem Kongress der Vereinigten Staaten von Amerika zu übermitteln.