P7_TA(2011)0323

Datenschutz in der Europäischen Union

Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI))

Das Europäische Parlament,

– unter Hinweis auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8, und auf die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), insbesondere auf Artikel 8 zum Schutz des Privat- und Familienlebens und auf Artikel 13 zum Recht auf einen wirksamen Rechtsbehelf,

– unter Hinweis 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[1],

– unter Hinweis auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[2],

– unter Hinweis auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[3],

– 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 (Datenschutzrichtlinie für elektronische Kommunikation)[4],

– unter Hinweis auf das Übereinkommen Nr. 108 des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, das mit der Richtlinie 95/46/EG weiterentwickelt wird, und auf das Zusatzprotokoll zu diesem Übereinkommen vom 8. November 2001 betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr sowie auf die Empfehlungen des Ministerkomitees an die Mitgliedstaaten, insbesondere die Empfehlung Nr. R (87)15 über die Nutzung personenbezogener Daten im Polizeibereich und die Empfehlung CM/Rec.(2010)13 betreffend den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling,

– unter Hinweis auf die Leitlinien für die Regelung personenbezogener Datenbanken, die

---

1 ABl. L 281 vom 23.11.1995, S. 31.
2 ABl. L 350 vom 30.12.2008, S. 60.
3 ABl. L 8 vom 12.1.2001, S. 1.
4 ABl. L 201 vom 31.7.2002, S. 37.

1990 von der Generalversammlung der Vereinten Nationen herausgegeben wurden,

– in Kenntnis der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Gesamtkonzept für den Datenschutz in der Europäischen Union (KOM(2010)0609),

– in Kenntnis der Schlussfolgerungen des Rates zur Mitteilung der Kommission zum Gesamtkonzept für den Datenschutz in der Europäischen Union[1],

– in Kenntnis der Stellungnahme des Europäischen Datenschutzbeauftragten vom 14. Januar 2011 zu der Mitteilung der Kommission zum Gesamtkonzept für den Datenschutz in der Europäischen Union,

– in Kenntnis des Gemeinsamen Beitrags der Arbeitsgruppe Polizei und Justiz der Artikel-29-Datenschutzgruppe zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten mit dem Titel „Die Zukunft des Datenschutzes“[2],

– in Kenntnis der Stellungnahme 8/2010 der Artikel-29-Datenschutzgruppe zu dem anwendbaren Recht[3],

– unter Hinweis auf seine früheren Entschließungen zum Datenschutz und seine Entschließung zum Stockholm-Programm[4],

– gestützt auf Artikel 48 seiner Geschäftsordnung,

– in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres sowie der Stellungnahmen des Ausschusses für Industrie, Forschung und Energie, des Ausschusses für Binnenmarkt und Verbraucherschutz, des Ausschusses für Kultur und Bildung sowie des Rechtsausschusses (A7-0244/2011),

A. in der Erwägung, dass die Datenschutzrichtlinie 95/46/EG und die Richtlinie mit dem EU-Telekommunikationspaket 2009/140/EG den freien Verkehr personenbezogener Daten innerhalb des Binnenmarktes ermöglichen,

B. in der Erwägung, dass Datenschutzvorschriften in der EU, in den Mitgliedstaaten und darüber hinaus eine rechtliche Tradition entwickelt haben, diese es zu bewahren und weiterzuentwickeln gilt,

---

1 3071. Tagung des Rates „Justiz und Inneres“ in Brüssel, 24. und 25. Februar 2011, zugänglich unter: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

2 02356/09/EN WP 168.

3 0836/10/EN WP 179.

4 Einige Beispiele: Standpunkt des Europäischen Parlaments vom 23. September 2008 zu dem Entwurf eines Rahmenbeschlusses des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. C 8 E vom 14.1.2010, S. 138); Empfehlung des Europäischen Parlaments vom 26. März 2009 an den Rat zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (ABl. C 117 E vom 6.5.2010, S. 206); Entschließung des Europäischen Parlaments vom 25. November 2009 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat – Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger – Stockholm-Programm (ABl. C 285 E vom 21.10.2010, S. 12).

C. in der Erwägung, dass der Kerngrundsatz der Richtlinie 95/46/EG weiterhin gültig ist, dass jedoch unterschiedliche Ansätze der Mitgliedstaaten bei seiner Umsetzung und Durchsetzung festgestellt worden sind; in der Erwägung, dass sich die EU – nach einer gründlichen Folgenabschätzung – einen umfassenden, kohärenten und modernen Rahmen auf hohem Niveau schaffen muss, mit dem die Grundrechte des Einzelnen, insbesondere die Privatsphäre, bei der Verarbeitung personenbezogener Daten von Einzelpersonen innerhalb und außerhalb der EU unter allen Umständen wirksam geschützt werden, um die zahlreichen Herausforderungen, die mit dem Datenschutz verbunden sind, wie etwa diejenigen, die sich durch die Globalisierung, die technologische Entwicklung, verstärkte Online-Aktivitäten, Nutzungen im Zusammenhang mit immer mehr Aktivitäten und Sicherheitsbedenken (d. h. Bekämpfung des Terrorismus) ergeben, zu bewältigen; in der Erwägung, dass ein Rahmen für den Datenschutz wie dieser die Rechtssicherheit erhöhen, den Verwaltungsaufwand auf ein Minimum reduzieren, gleiche Wettbewerbsbedingungen für die Wirtschaftsakteure gewährleisten, dem digitalen Binnenmarkt Dynamik verleihen und das Vertrauen in das Verhalten der für die Datenverarbeitung Verantwortlichen und Vollzugsbehörden herausbilden kann,

D. in der Erwägung, dass Verstöße gegen Datenschutzbestimmungen zu ernsthaften Risiken für die Grundrechte des Einzelnen und für die Werte der Mitgliedstaaten führen können, so dass die Union und die Mitgliedstaaten wirksame Maßnahmen gegen solche Verstöße ergreifen müssen; in der Erwägung, dass solche Verstöße zu einem Mangel an Vertrauen des Einzelnen führen, der die zweckdienliche Nutzung der neuen Technologien schwächt, und in der Erwägung, dass die unsachgemäße und missbräuchliche Verwendung von personenbezogenen Daten daher mit angemessenen, harten und abschreckenden Sanktionen einschließlich strafrechtlicher Sanktionen geahndet werden sollte,

E. in der Erwägung, dass andere in der Charta verankerte wichtige Grundrechte und andere Ziele der EU-Verträge wie das Recht auf freie Meinungsäußerung und Informationsfreiheit sowie der Grundsatz der Transparenz bei der Gewährleistung des Grundrechts des Schutzes personenbezogener Daten uneingeschränkt berücksichtigt werden müssen,

F. in der Erwägung, dass die neue Rechtsgrundlage in Artikel 16 AEUV und die Anerkennung des Rechts auf Schutz personenbezogener Daten in Artikel 8 und des Rechts auf Achtung des Privat- und Familienlebens in Artikel 7 der Charta der Grundrechte als eigenständige Rechte ein Gesamtkonzept für den Datenschutz auf allen Gebieten, auf denen persönliche Daten verarbeitet werden, einschließlich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, auf dem Gebiet der Gemeinsamen Außen- und Sicherheitspolitik, unbeschadet der spezifischen Bestimmungen in Artikel 39 EUV, und auf dem Gebiet der Datenverarbeitung durch die Organe und Einrichtungen der EU bedingungslos erfordern und unterstützen,

G. in der Erwägung, dass es von ausschlaggebender Bedeutung ist, bei der Prüfung legislativer Lösungen verschiedene wesentliche Elemente zu berücksichtigen, d. h. den wirksamen Schutz unter allen Umständen, unabhängig von politischen Präferenzen innerhalb eines bestimmten Zeitraums; in der Erwägung, dass der Rahmen über einen langen Zeitraum hinweg stabil sein muss, wobei Einschränkungen der Wahrnehmung des Rechts – soweit erforderlich – nur ausnahmsweise und unter strikter Beachtung des Gebots der Erforderlichkeit und Verhältnismäßigkeit erfolgen dürfen und nie die wesentlichen Elemente des Rechts als solches betreffen dürfen,

H. in der Erwägung, dass die Sammlung, die Auswertung, der Austausch und der Missbrauch von Daten sowie das Risiko der Erstellung von Profilen, die durch technische Entwicklungen möglich geworden sind, beispiellose Ausmaße angenommen haben und daher strenger Datenschutzregelungen wie etwa der Bestimmung des anwendbaren Rechts und der Festlegung der Verantwortlichkeiten aller betroffenen Parteien im Hinblick auf die Umsetzung der Datenschutzvorschriften der EU bedürfen; in der Erwägung, dass immer häufiger Kundenkarten (Club-Karten, Bonuskarten, Vorteilskarten usw.) von Unternehmen und im Handel zum Einsatz kommen, die zur Herstellung von Verbraucherprofilen genutzt werden oder werden können,

I. in der Erwägung, dass Bürger Online-Käufe nicht mit der gleichen Sicherheit tätigen wie offline, da Befürchtungen im Hinblick auf Identitätsdiebstahl bestehen und ein Mangel an Transparenz hinsichtlich der Frage besteht, wie ihre persönlichen Informationen verarbeitet und verwendet werden,

J. in der Erwägung, dass Technologien es in zunehmendem Maße ermöglichen, personenbezogene Daten an jedem Ort und zu jeder Zeit in vielen verschiedenen Formen zu erstellen, zu versenden, zu verarbeiten und zu speichern; in der Erwägung, dass es vor diesem Hintergrund von ausschlaggebender Bedeutung ist, dass Betroffene die wirksame Kontrolle über ihre eigenen Daten behalten,

K. in der Erwägung, dass das Grundrecht auf Datenschutz und auf Privatsphäre den Schutz von Personen vor möglicher Überwachung sowie vor Missbrauch ihrer Daten durch den Staat selbst und durch privatrechtliche Einrichtungen umfasst,

L. in der Erwägung, dass Privatsphäre und Sicherheit möglich sind und beide von ausschlaggebender Bedeutung für die Bürger sind, so dass es nicht notwendig ist, zwischen Freiheit und Sicherheit zu entscheiden,

M. in der Erwägung, dass Kinder besonderen Schutz genießen müssen, da sie sich der Risiken, Folgen, Garantien und Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sein dürften; in der Erwägung, dass junge Leute personenbezogene Daten auf den Internetseiten sich schnell im Internet verbreitender sozialer Netzwerke preisgeben,

N. in der Erwägung, dass eine wirksame Kontrolle durch die betroffene Person und die nationalen Datenschutzbehörden Transparenz im Verhalten der für die Datenverarbeitung Verantwortlichen erfordert,

O. in der Erwägung, dass nicht alle für die Datenverarbeitung Verantwortlichen Online-Unternehmen sind und daher neue Datenschutzregeln sowohl das Online- als auch das Offline-Umfeld umfassen müssen, wobei mögliche Unterschiede zwischen ihnen zu berücksichtigen sind,

P. in der Erwägung, dass die einzelstaatlichen Datenschutzbehörden in den 27 Mitgliedstaaten sehr unterschiedlichen Regelungen unterworfen sind, insbesondere im Hinblick auf Status, Ressourcen und Befugnisse,

Q. in der Erwägung, dass eine strenge europäische und internationale Datenschutzregelung die notwendige Grundlage für den grenzüberschreitenden Strom personenbezogener Daten ist; in der Erwägung, dass die gegenwärtigen Unterschiede im Recht und in der Durchsetzung des Datenschutzes den Schutz der Grundrechte und die individuellen Freiheiten, die

Rechtssicherheit und die Klarheit in den vertraglichen Beziehungen, die Entwicklung des e-Handels und der e-Geschäfte, das Vertrauen der Verbraucher in das System, grenzüberschreitende Transaktionen, die globale Wirtschaft und den europäischen Binnenmarkt beeinflussen; in der Erwägung, dass in diesem Zusammenhang der Datenaustausch wichtig für die Ermöglichung und Gewährleistung der öffentlichen Sicherheit auf nationaler und internationaler Ebene ist; in der Erwägung, dass Notwendigkeit, Verhältnismäßigkeit, Zweckbeschränkung, Aufsicht und Angemessenheit Voraussetzungen für den Austausch sind,

R. in der Erwägung, dass die derzeitigen Regelungen und Bedingungen für die Übermittlung personenbezogener Daten von der EU in Drittstaaten zu unterschiedlichen Ansätzen und Praktiken in den verschiedenen Mitgliedstaaten geführt haben; in der Erwägung, dass es unabdingbar ist, dass die Datenschutzrechte der betroffenen Personen bei der Übermittlung und Verarbeitung von personenbezogenen Daten in Drittstaaten in vollem Umfang durchgesetzt werden,

Volle Verpflichtung zu einem Gesamtkonzept

1. begrüßt nachdrücklich und unterstützt die Mitteilung der Kommission zum Gesamtkonzept für den Datenschutz in der Europäischen Union und ihren Schwerpunkt auf der Stärkung bestehender Übereinkünfte, wobei neue Grundsätze und Mechanismen dargestellt und Kohärenz und hohe Standards des Datenschutzes innerhalb der neuen Struktur gewährleistet werden, die durch das Inkrafttreten des Vertrags von Lissabon (Artikel 16 AEUV) und die mittlerweile rechtsverbindliche Charta der Grundrechte, insbesondere ihren Artikel 8, vorgesehen sind;

2. betont, dass die Standards und Grundsätze der Richtlinie 95/46/EG einen idealen Ausgangspunkt darstellen und als Teil eines modernen Datenschutzrechts weiterentwickelt, erweitert und gestärkt werden sollten;

3. unterstreicht die Bedeutung von Artikel 9 der Richtlinie 95/46/EG, der die Mitgliedstaaten verpflichtet, Ausnahmen von Datenschutzbestimmungen vorzusehen, wenn personenbezogene Daten nur für journalistische Zwecke oder künstlerischen oder literarischen Ausdruck verwendet werden; fordert die Kommission in diesem Zusammenhang auf zu gewährleisten, dass diese Ausnahmen beibehalten werden, und dass im Lichte neuer Vorschriften alle Anstrengungen unternommen werden, um die Notwendigkeit einer Weiterentwicklung dieser Ausnahmen im Sinne des Schutzes der Pressefreiheit zu bewerten;

4. unterstreicht, dass der technologisch neutrale Ansatz der Richtlinie 95/46/EG als Grundsatz eines neuen Rahmens beibehalten werden sollte;

5. erkennt an, dass die technologische Entwicklung auf der einen Seite neue Gefahren für den Schutz personenbezogener Daten geschaffen und auf der anderen Seite zu einer enormen Zunahme der Nutzung von Informationstechnologien für den täglichen und normalerweise harmlosen Gebrauch geführt hat; erkennt ferner an, dass die Entwicklung eine genaue Bewertung der derzeit geltenden Datenschutzvorschriften erforderlich macht, um zu gewährleisten, dass die Vorschriften erstens weiterhin ein hohes Schutzniveau garantieren, zweitens weiterhin einen fairen Ausgleich zwischen dem Recht auf Schutz personenbezogener Daten und dem Recht auf Meinungs- und Informationsfreiheit gewährleisten und drittens die Vorschriften nicht unnötigerweise die tägliche,

normalerweise harmlose Verarbeitung von personenbezogenen Daten behindern;

6. hält es für dringend geboten, den Anwendungsbereich der allgemeinen Datenschutzbestimmungen auf die Bereiche der polizeilichen und justiziellen Zusammenarbeit auszudehnen, und zwar auch bei innerstaatlicher Datenverarbeitung unter besonderer Berücksichtigung der fragwürdigen Tendenz zur systematischen Wiederverwendung personenbezogener Daten des Privatsektors zu Zwecken der Strafverfolgung bei – unter strikter Beachtung des Gebots der Erforderlichkeit und Verhältnismäßigkeit in einer demokratischen Gesellschaft erfolgender – gleichzeitiger Zulassung eng begrenzter und harmonisierter Einschränkungen bestimmter Datenschutzrechte des Einzelnen;

7. betont die Notwendigkeit, die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Europäischen Union gemäß der Verordnung (EG) Nr. 45/2001 in den Anwendungsbereich des neuen Rahmens einzubeziehen;

8. erkennt an, dass zusätzliche verstärkte Maßnahmen benötigt werden könnten, um festzulegen, wie die allgemeinen Grundsätze, die durch den umfassenden Rahmen geschaffen werden, auf die Tätigkeiten spezifischer Sektoren und die Datenverarbeitung Anwendung finden, wie dies bereits bei der Datenschutzrichtlinie für elektronische Kommunikation der Fall war; besteht jedoch darauf, dass durch die sektorspezifischen Regelungen unter keinen Umständen das durch die Rahmengesetzgebung gewährleistete Schutzniveau abgesenkt und die Abweichungen von den allgemeinen Datenschutzgrundsätzen als eng begrenzte Ausnahmefälle unter Beachtung des Gebots der Erforderlichkeit und Rechtmäßigkeit genau definiert werden sollten;

9. fordert die Kommission auf zu gewährleisten, dass die gegenwärtige Überprüfung des Datenschutzrechts der EU Folgendes ermöglichen wird:

   – die volle Harmonisierung auf höchstem Niveau, die für Rechtssicherheit und ein einheitliches hohes Schutzniveau für den Einzelnen unter allen Umständen sorgt;

   – die weitere Klärung der Regelungen für das anwendbare Recht, um unabhängig vom geografischen Standort des für die Datenverarbeitung Verantwortlichen ein einheitliches Schutzniveau für den Einzelnen durchzusetzen, wozu auch die Durchsetzung der Datenschutzvorschriften durch Behörden oder vor Gerichten zählt;

10. ist der Ansicht, dass durch das überarbeitete Datenschutzrecht das Recht auf Privatsphäre und auf Datenschutz umfassend umgesetzt werden sollte und gleichzeitig bürokratische und finanzielle Belastungen auf ein Minimum begrenzt und Instrumente angeboten werden sollten, die es als eine Einheit wahrgenommenen Konzernen erlauben, als eine Einheit zu handeln, und nicht wie eine Vielzahl von getrennten Unternehmen; fordert die Kommission auf, Folgenabschätzungen durchzuführen und die Kosten neuer Maßnahmen genau zu prüfen;

Stärkung der Rechte des Einzelnen

11. fordert die Kommission auf, bestehende Grundsätze und Bestandteile auszubauen, wie etwa Transparenz, Datensparsamkeit, Zweckbindung, die vorherige und ausdrückliche Zustimmung in Kenntnis der Sachlage, die Meldung von Verstößen gegen die Datensicherheit und die Rechte der betroffenen Personen, wie sie in der Richtlinie

95/46/EG dargelegt sind, wobei ihre Umsetzung in den Mitgliedstaaten verbessert wird, insbesondere im Hinblick auf das globale Online-Umfeld;

12. betont, dass die Zustimmung nur dann gültig ist, wenn sie unmissverständlich, in Kenntnis der Sachlage, frei, für den konkreten Fall und ausdrücklich erfolgt und dass angemessene Mechanismen umgesetzt werden müssen, um die Zustimmung der Nutzer oder die Widerrufung dieser Zustimmung zu erfassen;

13. weist darauf hin, dass die freiwillige Zustimmung im Bereich der Arbeitsverträge nicht vorausgesetzt werden kann;

14. ist besorgt über die missbräuchlichen Praktiken im Bereich der verhaltensorientierten Online-Werbung und weist darauf hin, dass in der Datenschutzrichtlinie für elektronische Kommunikation festgelegt ist, dass die vorherige ausdrückliche Zustimmung der betreffenden Person vorliegen muss, bevor ihr Cookies angezeigt werden und ihr Surfverhalten weiter mit dem Ziel beobachtet wird, ihr personalisierte Anzeigen zuzusenden;

15. unterstützt uneingeschränkt die Einführung eines allgemeinen Transparenzgrundsatzes wie auch die Verwendung von Technologien zur Verbesserung der Transparenz und die Entwicklung von standardisierten Datenschutzhinweisen, die dem Einzelnen eine Kontrolle über seine Daten ermöglicht; betont, dass Informationen über die Datenverarbeitung klar und einfach abgefasst sowie leicht verständlich und zugänglich sein müssen;

16. betont ferner, wie wichtig es ist, die Mittel zur und die Sensibilisierung für die Ausübung des Rechts auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung zu verbessern und das sogenannte Recht auf Vergessen („right to be forgotten“)[1] zu präzisieren und zu kodifizieren und die Datenübertragbarkeit[2] zu ermöglichen, wobei zu gewährleisten ist, dass die vollständige technische und organisatorische Durchführbarkeit der Wahrnehmung dieser Rechte entwickelt wird und vorhanden ist; unterstreicht, dass Nutzer ausreichende Kontrolle über ihre Online-Daten haben müssen, um verantwortlich vom Internet Gebrauch zu machen;

17. betont, dass die Bürger in der Lage sein müssen, ihre Datenrechte gebührenfrei wahrzunehmen; fordert die Unternehmen auf, von Versuchen Abstand zu nehmen, das Recht auf Zugang, Änderung oder Löschung personenbezogener Daten unnötig einzuschränken; betont, dass die betroffene Person in die Lage versetzt werden muss, zu jeder Zeit zu wissen, welche Daten durch wen, wann, zu welchem Zweck, für welchen Zeitraum gespeichert wurden und wie diese verarbeitet werden, und dass die betroffene Person die Löschung, Berichtigung und Sperrung von Daten unbürokratisch erwirken können muss und dass die betroffene Person über jeden Missbrauch von Daten und jeden Verstoß gegen die Datensicherheit zu informieren ist; fordert ferner, dass Daten auf Antrag der betroffenen Person offengelegt und spätestens dann gelöscht werden, wenn die betroffene Person dies fordert; unterstreicht die Notwendigkeit, den Betroffenen klar den

---

[1] Die einschlägigen Elemente, die diesem Recht zugrunde liegen, müssen klar und genau festgelegt werden.

[2] Die Übertragbarkeit personenbezogener Daten wird das reibungslose Funktionieren sowohl des Binnenmarktes als auch des Internet und seiner charakteristischen Offenheit und Interkonnektivität erleichtern.

Grad des Datenschutzes in Drittstaaten mitzuteilen; betont, dass das Recht auf Zugang nicht nur den umfassenden Zugang zu den verarbeiteten Daten der betroffenen Person selbst, einschließlich der Quelle und der Empfänger, sondern auch verständliche Informationen über die jeder automatischen Verarbeitung zugrundeliegende Logik einschließt; betont, dass Letzteres angesichts der Erstellung von Profilen und gezielter Datenextraktion („data mining“) immer wichtiger werden wird;

18. erinnert daran, dass das Erstellen von Profilen („Profiling“) in der „digitalen Welt“ ein bedeutender Trend ist, was nicht zuletzt auf die wachsende Bedeutung sozialer Netzwerke und integrierter Internet-Geschäftsmodelle zurückzuführen ist; fordert die Kommission daher auf, Regelungen zum Profiling einzubeziehen und gleichzeitig die Begriffe „Profil“ und „Profiling“ eindeutig zu definieren;

19. bekräftigt, dass die Pflichten der für die Datenverarbeitung Verantwortlichen, den betroffenen Personen Informationen bereitzustellen, gestärkt werden müssen, und begrüßt, dass Sensibilisierungsmaßnahmen sowohl für die Öffentlichkeit im Allgemeinen als auch für junge Menschen im Besonderen in der Mitteilung besondere Aufmerksamkeit gewidmet wird; betont, dass im Umgang mit schutzbedürftigen Personen und insbesondere mit Kindern und älteren Menschen spezielle Verfahren erforderlich sind; ermutigt die verschiedenen Akteure, solche Sensibilisierungsmaßnahmen durchzuführen, und unterstützt den Vorschlag der Kommission, Sensibilisierungsmaßnahmen zum Datenschutz aus dem Unionshaushalt mitzufinanzieren; fordert, dass in allen Mitgliedstaaten für eine effiziente Verbreitung von Informationen über die Rechte und Pflichten natürlicher und juristischer Personen im Hinblick auf die Erhebung, Verarbeitung, Speicherung und Weitergabe von personenbezogenen Daten gesorgt wird;

20. weist darauf hin, dass für schutzbedürftige Personen, insbesondere Kinder, spezifische Formen des Schutzes bereitgestellt werden müssen, vor allem indem ein hoher Datenschutzstandard und die Durchführung geeigneter und spezifischer Maßnahmen vorgeschrieben werden, damit ihre personenbezogenen Daten geschützt werden;

21. betont, wie wichtig es ist, dass – unter anderem im Lichte des zunehmenden Zugangs von Kindern zum Internet und zu digitalen Inhalten – mit dem Datenschutzrecht die Notwendigkeit anerkannt wird, Kinder und Minderjährige besonders zu schützen, und hebt hervor, dass Medienkompetenz Teil der formalen Bildung werden muss, damit Kinder und Minderjährige lernen, wie sie sich in der Online-Umgebung verantwortungsvoll verhalten können; vertritt in diesem Zusammenhang die Auffassung, dass Vorschriften über die Sammlung und Weiterverarbeitung der Daten von Kindern, die Verstärkung des Zweckbindungsgrundsatzes in Bezug auf die Daten von Kindern und darüber, wie die Zustimmung von Kindern eingeholt wird, und über den Schutz vor verhaltensorientierter Online-Werbung besondere Aufmerksamkeit gewidmet werden sollte[1];

22. unterstützt weitere Klarstellungen und die Stärkung der Garantien im Hinblick auf die Verarbeitung sensibler Daten und fordert ein Nachdenken über die Notwendigkeit, sich mit neuen Datenkategorien wie Gendaten und biometrischen Daten – insbesondere angesichts

---

1 Eine Altersgrenze für Kinder, unter der die Zustimmung der Eltern eingeholt wird, und Verfahren zur Überprüfung des Alters könnten in Betracht gezogen werden.

technologischer (etwa Cloudcomputing) und gesellschaftlicher Entwicklungen – zu beschäftigen;

23. hebt hervor, dass personenbezogene Daten in Bezug auf die berufliche Situation des Nutzers, die dem Arbeitgeber zur Verfügung gestellt werden, nicht ohne die vorherige Zustimmung des Betroffenen veröffentlicht oder an Dritte weitergegeben werden dürfen;

Weitere Stärkung der Binnenmarktdimension und Sicherung der besseren Durchsetzung von Datenschutzvorschriften

24. stellt fest, dass der Datenschutz im Binnenmarkt eine immer größere Rolle spielen sollte, und betont, dass der wirksame Schutz des Rechts auf Privatsphäre von wesentlicher Bedeutung dafür ist, das Vertrauen des Einzelnen zu gewinnen, das erforderlich ist, um das gesamte Wachstumspotenzial des digitalen Binnenmarktes auszuschöpfen; erinnert die Kommission daran, dass gemeinsame Grundsätze und Regeln für Waren wie für Dienstleistungen eine Vorbedingung für einen digitalen Binnenmarkt sind, da Dienstleistungen einen wichtigen Teil des digitalen Marktes ausmachen;

25. fordert die Kommission erneut auf, die Vorschriften in Bezug auf das anwendbare Recht auf dem Gebiet des Schutzes personenbezogener Daten zu klären;

26. hält es für wesentlich, die Verpflichtungen der für die Datenverarbeitung Verantwortlichen weiter auszudehnen, um die Einhaltung des Datenschutzrechts zu gewährleisten, indem unter anderem aktive Maßnahmen ergriffen und Verfahren bereitgestellt werden, und begrüßt die in der Mitteilung der Kommission vorgeschlagenen anderen Wege;

27. erinnert in diesem Zusammenhang daran, dass den für die Datenverarbeitung Verantwortlichen, für die das Berufsgeheimnis betreffende Verpflichtungen gelten, besondere Aufmerksamkeit zu widmen ist, und dass für diese der Aufbau spezieller Strukturen der Datenschutzaufsicht in Erwägung gezogen werden sollte;

28. begrüßt und unterstützt die Erwägungen der Kommission zur Einführung eines Rechenschaftsgrundsatzes, da dies von entscheidender Bedeutung dafür ist zu gewährleisten, dass die für die Datenverarbeitung Verantwortlichen ihrer Verantwortung entsprechend tätig werden; fordert die Kommission gleichzeitig auf, sorgfältig zu untersuchen, wie dieser Grundsatz in die Praxis umgesetzt werden könnte, und festzustellen, welche Folgen dieser hätte;

29. begrüßt die Möglichkeit, die Ernennung eines Datenschutzbeauftragten für obligatorisch zu erklären, da die Erfahrung der EU-Mitgliedstaaten, die bereits einen Datenschutzbeauftragten ernannt haben, zeigt, dass dieses Konzept erfolgreich ist; weist jedoch darauf hin, dass dies im Hinblick auf Klein- und Kleinstunternehmen sorgfältig geprüft werden muss, um zu vermeiden, dass ihnen hohe Kosten oder Belastungen auferlegt werden;

30. begrüßt in diesem Zusammenhang auch die Anstrengungen zur Vereinfachung und Harmonisierung der derzeitigen Melderegelung;

31. hält es für wesentlich, die Folgenabschätzung für die Privatsphäre obligatorisch zu gestalten, um die Risiken für die Privatsphäre festzustellen, Probleme im Voraus zu erkennen und zukunftsweisende Lösungen vorzuschlagen;

32. hält es für entscheidend, dass die Rechte der Betroffenen einklagbar sind; stellt fest, dass mit der Einführung von Sammelklagen Einzelpersonen ein Instrument erlangen könnten, mit dem sie ihre Datenrechte kollektiv schützen und Schadenersatz für Schäden infolge von Datenschutzverstößen fordern könnten; weist allerdings darauf hin, dass es hierbei Beschränkungen geben müsste, um Missbrauch zu verhindern; ruft die Kommission auf, das Verhältnis zwischen dieser Mitteilung zum Datenschutz und der derzeit laufenden öffentlichen Konsultation zu Sammelklagen darzulegen; fordert daher ein kollektives Rechtsdurchsetzungsverfahren im Fall der Verletzung von Datenschutzbestimmungen, damit betroffene Personen Schadensersatz erlangen können;

33. unterstreicht die Notwendigkeit einer angemessenen harmonisierten Durchsetzung in der gesamten EU; fordert die Kommission auf, in ihrem Legislativvorschlag harte und abschreckende Sanktionen einschließlich strafrechtlicher Sanktionen für die unsachgemäße und missbräuchliche Verwendung von personenbezogenen Daten vorzusehen;

34. fordert die Kommission auf, einen obligatorischen Mechanismus zur Anzeige von Verletzungen des Schutzes personenbezogener Daten einzuführen, indem dieser auf andere Bereiche als den der Telekommunikation ausgedehnt wird, wobei sicherzustellen ist, dass der Mechanismus erstens nicht routinemäßig bei allen Arten von Verstößen ausgelöst wird, sondern hauptsächlich nur bei denen, die negative Auswirkungen auf den Einzelnen haben können, und dass zweitens alle Verletzungen ohne Ausnahme protokolliert werden und den Datenschutzbehörden oder anderen Aufsichts- und Prüfungsbehörden zur Verfügung stehen, um gleiche Wettbewerbsbedingungen und einen einheitlichen Schutz für alle Bürger zu gewährleisten;

35. sieht in den Konzepten „Privacy by Design“ und „Privacy by Default“ eine Stärkung des Datenschutzes und unterstützt ihre konkrete Anwendung und weitere Entwicklung sowie die Notwendigkeit, den Einsatz von Technologien zur Stärkung der Privatsphäre zu fördern; betont, dass die Umsetzung des Konzepts „Privacy by Design“ auf solide und konkrete Kriterien und Definitionen gestützt werden muss, um das Recht des Einzelnen auf Privatsphäre und Datenschutz zu schützen und Rechtssicherheit, Transparenz, gleiche Wettbewerbsbedingungen und Freizügigkeit zu gewährleisten; ist der Auffassung, dass „Privacy by Design“ auf dem Grundsatz der Datensparsamkeit beruhen sollte, d. h. alle Produkte, Dienstleistungen und Systeme sollten so konzipiert sein, dass sie nur die personenbezogenen Daten sammeln, verwenden und übermitteln, die für ihr Funktionieren unbedingt erforderlich sind;

36. stellt fest, dass die Entwicklung und der breitere Einsatz von Cloud Computing neue Herausforderungen im Hinblick auf die Privatsphäre und den Schutz personenbezogener Daten aufwerfen; fordert deshalb eine Klärung der Kapazitäten der für die Datenverarbeitung Verantwortlichen, der Datenverarbeiter und der Datenbankanbieter, um die entsprechenden rechtlichen Verantwortlichkeiten besser zuzuweisen und dafür zu sorgen, dass die Betroffenen wissen, wo ihre Daten gespeichert werden, wer Zugang zu ihren Daten hat, wer über die Verwendung der personenbezogenen Daten beschließt und welche Art von Backup- und Recovery-Prozessen vorhanden sind;

37. fordert die Kommission daher auf, bei der Revision der Richtlinie 95/46/EG Fragen des Datenschutzes in Verbindung mit Cloud Computing gebührend Rechnung zu tragen und zu gewährleisten, dass die Datenschutzvorschriften auf alle betroffenen Parteien, einschließlich von Betreibern im Bereich der Telekommunikation und Betreibern

außerhalb des Bereichs der Telekommunikation, Anwendung finden;

38. ruft die Kommission dazu auf, bei allen Akteuren des Internet das Verantwortungsgefühl im Hinblick auf personenbezogene Daten zu stärken, und fordert insbesondere, dass Werbeagenturen und Web Publisher Internetnutzer vor der Sammlung von Daten zu ihrer Person explizit darüber aufklären müssen;

39. begrüßt die jüngst unterzeichnete Vereinbarung über einen Rahmen für die Datenschutz-Folgenabschätzung (PIA) bei Anwendungen der Funkfrequenzkennzeichnung (RFID), der darauf abzielt, den Schutz der Privatsphäre der Verbraucher zu gewährleisten, bevor RFID-Tags auf einen bestimmten Markt gebracht werden;

40. begrüßt die Bemühungen zur weiteren Stärkung der Selbstregulierungsinitiativen – wie Verhaltenskodizes – und die Überlegungen zur Einführung von freiwilligen EU-Zertifizierungsregelungen als Ergänzungen zu legislativen Maßnahmen, wobei das Datenschutzmodell der EU weiterhin auf Rechtsvorschriften basiert, die hohe Garantien festlegen; fordert die Kommission auf, eine Folgenabschätzung der Selbstregulierungsinitiativen als Instrumente für eine bessere Durchsetzung von Datenschutzvorschriften durchzuführen;

41. ist der Ansicht, dass die Integrität und Glaubwürdigkeit, Technologieneutralität, globale Anerkennung und Erschwinglichkeit jedes Zertifizierungs- oder Siegelsystems sichergestellt werden müssen, damit keine Zutrittsschranken geschaffen werden;

42. befürwortet die weitere Klarstellung, Stärkung und Harmonisierung der Rechtsstellung und der Befugnisse der nationalen Datenschutzbehörden und die Prüfung von Wegen, wie eine kohärentere Anwendung der Datenschutzvorschriften der EU im gesamten Binnenmarkt sichergestellt werden kann; hebt ferner hervor, wie wichtig es ist, die Kohärenz zwischen den Zuständigkeiten des Europäischen Datenschutzbeauftragten, der nationalen Datenschutzbehörden und der Datenschutzgruppe „Artikel 29“ zu gewährleisten;

43. unterstreicht in diesem Zusammenhang, dass die Rolle und die Befugnisse der Datenschutzgruppe „Artikel 29“ gestärkt werden sollten, um die Koordination und Zusammenarbeit zwischen den Datenschutzbehörden der Mitgliedstaaten zu verbessern, insbesondere im Hinblick auf die Sicherung einer einheitlichen Anwendung der Datenschutzbestimmungen;

44. fordert die Kommission auf, in dem neuen Rechtsrahmen den wesentlichen Begriff der Unabhängigkeit der nationalen Datenschutzbehörden in dem Sinne, dass eine Beeinflussung von außen unterbleibt, klarzustellen[1]; betont, dass den nationalen Datenschutzbehörden die erforderlichen Ressourcen gewährt und ihnen harmonisierte Befugnisse zur Durchführung von Untersuchungen und Verhängung von Sanktionen übertragen werden sollten;

Stärkung der globalen Dimension des Datenschutzes

45. fordert die Kommission auf, die bestehenden Verfahren für den internationalen Datentransfer – im Wege rechtsverbindlicher Vereinbarungen und verbindlicher unternehmensinterner Vorschriften – zu straffen und zu verstärken und die ehrgeizigen

[1] Im Einklang mit Artikel 16 AEUV und Artikel 8 der Charta.

zentralen Elemente des Datenschutzes der EU auf der Basis der oben genannten Grundsätze im Bereich des Schutzes der personenbezogenen Daten für internationale Vereinbarungen zu definieren; betont, dass in den Abkommen der EU mit Drittstaaten über den Schutz personenbezogener Daten gewährleistet werden muss, dass für die Unionsbürger der gleiche Standard für den Schutz personenbezogener Daten gilt wie innerhalb der Europäischen Union;

46. ist der Ansicht, dass für das Verfahren der Kommission zur Prüfung der Angemessenheit weitere Klarstellungen, eine strengere Umsetzung und Durchsetzung sowie Überwachung von Vorteil wären und dass Kriterien und Anforderungen für die Bewertung des Datenschutzniveaus in einem Drittland oder in einer internationalen Organisation unter Berücksichtigung der neuen Gefahren für die Privatsphäre und die personenbezogenen Daten besser festgelegt werden sollten;

47. fordert die Kommission auf, die Wirksamkeit und die korrekte Anwendung der „Grundsätze des sicheren Hafens“ sorgfältig zu überprüfen;

48. begrüßt den Standpunkt der Kommission zur Gegenseitigkeit bei den Schutzniveaus für betroffene Personen, deren Daten in Drittländer ausgeführt oder dort aufbewahrt werden; fordert die Kommission auf, entschiedene Schritte hin zu einer verstärkten ordnungspolitischen Zusammenarbeit mit Drittstaaten zu ergreifen, um die anwendbaren Regeln und die Konvergenz der Datenschutzbestimmungen der EU und von Drittstaaten zu klären; fordert die Kommission auf, dies als vorrangiges Thema auf die Tagesordnung des neubelebten Transatlantischen Wirtschaftsrates zu setzen;

49. unterstützt die Anstrengungen der Kommission, die Zusammenarbeit mit Drittstaaten und internationalen Organisationen, einschließlich der Vereinten Nationen, des Europarats und der OECD sowie Normungsorganisationen wie dem Europäischen Komitee für Normung (CEN), der Internationalen Organisation für Normung (ISO), dem World Wide Web Consortium (W3C) und der Internet Engineering Task Force (IETF) zu verbessern; ermutigt dazu, internationale Standards[1] zu entwickeln und gleichzeitig sicherzustellen, dass Kohärenz zwischen den Initiativen für internationale Standards und laufende Revisionen in der EU, der OECD und im Europarat besteht;

o

o o

[1] Vgl. die Erklärung von Madrid vom Oktober 2009 mit dem Titel: „Global Privacy Standards for a Global World“ und die Resolution zu internationalen Standards, die von der 32. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 27. bis 29. Oktober 2010 in Jerusalem angenommen wurde.

50. beauftragt seinen Präsidenten, diese Entschließung dem Rat und der Kommission zu übermitteln.