

Stellungnahme des Europäischen Datenschutzbeauftragten zur künftigen Entwicklung des Raums der Freiheit, der Sicherheit und des Rechts

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr¹,

gestützt 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 Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr², insbesondere auf Artikel 41 Absatz 2 –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1. Diese Stellungnahme ist als Beitrag zur weiteren Entwicklung der EU-Politiken im Raum der Freiheit, der Sicherheit und des Rechts durch vollständige Integration des Schutzes der Privatsphäre und des Datenschutzes in die Tätigkeiten aller EU-Organe gedacht. Sie stellt die Reaktion auf zwei von der Kommission am 11. März 2014 angenommene Mitteilungen über die Zukunft des Bereichs Justiz und Inneres³, die Entschließung des Europäischen Parlaments vom 2. April 2014 zur Überarbeitung des Stockholmer Programms und Diskussionen im Rat dar, in denen es zum ersten Mal, wie in Artikel 68 AEUV vorgesehen, um die Festlegung strategischer Leitlinien durch den Europäischen Rat für die gesetzgeberische und operative Programmplanung geht.
2. Im Hinblick auf die Rolle der EU in den Bereichen Justiz und Inneres stehen wir an einem kritischen Punkt. Es rückt das Ende des im Vertrag von Lissabon festgelegten Übergangszeitraums näher, nach dessen Ablauf die Befugnisse der Kommission zur Einleitung von Vertragsverletzungsverfahren und die Befugnisse des Europäischen Gerichtshofs sich in vollem Umfang auch auf EU-Rechtsvorschriften über die polizeiliche

¹ ABl. L 281 vom 23.11.1995, S. 31.

² ABl. L 8 vom 12.1.2001, S. 1.

³ Siehe weiter unten Punkt [8] dieser Stellungnahme.

und justizielle Zusammenarbeit in Strafsachen erstrecken.⁴ Gemäß dem Vertrag ist die Charta der Grundrechte Bestandteil des Primärrechts, und der Europäische Gerichtshof hat in der jüngeren Vergangenheit in mehreren Urteilen die Grenzen des Handlungsspielraums des Gesetzgebers für den Fall abgesteckt, dass eine Maßnahme einen Eingriff in diese Rechte darstellt.⁵

3. Darüber hinaus haben in den vergangenen fünf Jahren Bedenken in Fragen der Privatsphäre und des Datenschutzes im Vergleich zu früher deutlich an Gewicht gewonnen. Im Januar 2012 legte die Kommission ein Paket zur Reform des Datenschutzrechts in der EU vor.⁶ Seit Juni 2013 haben Enthüllungen über die massenhafte Überwachung von Privatpersonen in der EU durch Nachrichtendienste der USA und anderer Länder das Vertrauen in die Vertraulichkeit personenbezogener Daten schwer beschädigt. Erst vor kurzem, im April 2014, hat der Gerichtshof in einem der beiden eben zitierten Urteile die Richtlinie über die Vorratsdatenspeicherung⁷ wegen ihrer übermäßigen Eingriffe in Grundrechte für ungültig erklärt. Jede datenschutzrechtliche Maßnahme auf EU-Ebene findet unterdessen weltweit Beachtung, wie es z. B. das Ausmaß der internationalen Berichterstattung und die umfangreiche Tätigkeit von Lobbyisten im Zusammenhang mit der Reform des Datenschutzregelwerks zeigen, die zur Einreichung rund 4 000 Änderungsanträgen im Verlauf der ersten Lesung im Europäischen Parlament führte.⁸
4. In dem von den strategischen Leitlinien abgedeckten Zeitraum dürften politische Entscheidungsträger und Gesetzgeber im Bereich Justiz und Inneres vor wachsenden rechtlichen, technologischen und gesellschaftlichen Herausforderungen stehen. Die neuen Leitlinien des Europäischen Rates bieten überdies Gelegenheit zur Bekräftigung der Absicht, das Vertrauen in die Fähigkeit der EU wiederherzustellen stärken, den Einzelnen wirksam zu schützen. Daher schlagen wir dem Europäische Rat vor, in den neuen Leitlinien ausdrücklich auf folgende Themen einzugehen:
 - a. die Verarbeitung der riesigen Mengen personenbezogener Daten, die in vielen Rechtsvorschriften und Politiken der EU im Bereich Freiheit, Sicherheit und Recht verlangt wird;

⁴ Die Übergangsbestimmungen gelten bis zum 1. Dezember 2014; Artikel 10, Protokoll Nr. 36 über die Übergangsbestimmungen, Anhang zum Vertrag von Lissabon.

⁵ Siehe in diesem Zusammenhang die Urteile des Gerichtshofs (Große Kammer) vom 9. November 2010 *Schecke und Eifert* (verbundene Rechtssachen C-92/09 und C-93/09) und insbesondere vom 8. April 2014 in *Digital Rights Ireland and Seitlinger* (verbundene Rechtssachen C-293/12 und C-594/12). In der ersten Rechtssache unterstrich der Gerichtshof die Notwendigkeit für den Gesetzgeber, bei einer bestimmten Maßnahme ausreichend weniger die Privatsphäre beeinträchtigende Alternativen in Erwägung zu ziehen.

⁶ KOM(2012) 11 endgültig und KOM(2012) 10 endgültig.

⁷ Richtlinie 2006/24/EG, ABl. L 105 vom 13.4.2006, S. 54.

⁸ Das Ergebnis der ersten Lesung im Europäischen Parlament war die legislative Entschließung vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (KOM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordentliches Gesetzgebungsverfahren: erste Lesung).

- b. die Fragilität aller Maßnahmen, die gegen Grundrechte verstoßen, wie in der Richtlinie über die Vorratsdatenspeicherung bestätigt wurde, die auch für andere derzeitige Initiativen wie das Paket „Intelligente Grenzen“⁹ und die verschiedenen Instrumente im Zusammenhang mit Fluggastdatensätzen gelten kann;¹⁰
 - c. die Bedeutung einer möglichst baldigen Annahme eines starken und modernisierten Datenschutzregelwerks in der EU, das auch als Richtschnur für die Außenpolitik der EU gelten sollte, und
 - d. das Erfordernis einer Berücksichtigung von Erwägungen zu Privatsphäre und Datenschutz bei der Ausarbeitung aller neuen Maßnahmen und Rechtsvorschriften im Raum der Freiheit, der Sicherheit und des Rechts.
5. Nachdem wir bereits vor fünf Jahren in einem ähnlichen Zusammenhang einen Beitrag geleistet haben, bieten wir in dieser Stellungnahme den EU-Organen als Teil eines neuen Konzepts für die Zusammenarbeit an, mit ihnen gemeinsam an einer Verbesserung der Rechtsvorschriften aus dem Blickwinkel des Datenschutzes zu arbeiten.¹¹

2. BETRACHTUNG DER ZUKUNFT DES RAUMS DER FREIHEIT, DER SICHERHEIT UND DES RECHTS AUS INSTITUTIONELLER SICHT

6. Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger („Stockholmer Programm“)¹², angenommen im Rahmen von Schlussfolgerungen des Europäischen Rates am 10./11. Dezember 2009, war die dritte für mehrere Jahre geltende Absichtserklärung in Folge im Bereich Justiz und Inneres.¹³ Es ging zurück auf eine Mitteilung der Kommission vom Juni 2009 mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“. In seiner am 13. Juli 2009 veröffentlichten Stellungnahme begrüßte der EDSB, dass die Kommission dem Schutz der Grundrechte und hier vor allem dem Schutz personenbezogener Daten in der Politik der EU in den Bereichen Staatsbürgerschaft, Justiz, Sicherheit, Asyl und Einwanderung großes Gewicht beimisst. Insbesondere begrüßten wir die Forderung nach einer umfassenden Datenschutzregelung für alle in die Zuständigkeit der EU fallenden Bereiche sowie die Bekräftigung grundlegender Prinzipien wie den der Zweckbindung. Die Kommission plante damals die Entwicklung eines „Europäischen Informationsmodells“ und einer „Europäischen Strategie für das Informationsmanagement“, von denen wir uns eine angemessene Berücksichtigung dieser Grundsätze und vorbildlichen Verfahrensweisen erhofften.

⁹ Siehe die Stellungnahme des EDSB vom 18. Juli 2013 zu den Vorschlägen für eine Verordnung über ein Einreise-/Ausreisensystem (EES) und für eine Verordnung über ein Registrierungsprogramm für Reisende (RTP).

¹⁰ Dazu gehört ein EU-System für Fluggastdatensätze (KOM(2011) 32 endgültig) und ein möglicher Vorschlag über die Übermittlung von Fluggastdaten an Drittstaaten (http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_home_004_transfer_pnr_data_3rd_countries_en.pdf [aufgerufen am 3. Juni 2014]).

¹¹ Siehe nähere allgemeine Ausführungen zu diesem Konzept im Strategiepapier des EDSB aus dem Jahr 2014 „The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience“ (Der EDSB als Berater von EU-Organen in Fragen von Politik und Gesetzgebung, gestützt auf zehnjährige Erfahrungen), einzusehen auf der Website des EDSB.

¹² ABl. C 155 vom 4.5.2010, S. 1.

¹³ KOM(2009) 262 endgültig.

7. Am 19./20. Dezember 2013 kündigte der Europäische Rat in Wahrnehmung seiner Aufgabe gemäß Artikel 68 AEUV zum ersten Mal nach den derzeitigen Verträgen seine Absicht an, „strategische Leitlinien für die gesetzgeberische und operative Programmplanung im Raum der Freiheit, der Sicherheit und des Rechts“ festzulegen („Post-Stockholm“).¹⁴
8. Am 11. März 2014 wurden zu diesen Themenkreisen zwei Mitteilungen der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen angenommen: In der ersten Mitteilung „Die EU-Justizagenda für 2020 – Stärkung von Vertrauen, Mobilität und Wachstum in der Union“¹⁵ ging es um die Konzepte der „Konsolidierung“ bestehender Maßnahmen, beispielsweise durch mehr Fortbildung von Richtern und Staatsanwälten, die „Kodifizierung“ von Zivil- und Handelsrecht, Verbraucherrechten und Strafrecht, und die Ermittlung von Maßnahmen zur „Ergänzung“ von gegenseitigem Vertrauen, Wirtschaftswachstum und Bürgerrechten. Die zweite Mitteilung „Ein offenes und sicheres Europa: Praktische Umsetzung“¹⁶ enthielt eher themenspezifische Vorschläge in den Bereichen legale Migration (wie Koordinierung von Bewertungen von Arbeitsmigration), illegale Migration, Änderung des EU-Visakodex, Asyl (wie gegenseitige Anerkennung von Entscheidungen) und Sicherheit (wie neue Gesetze zur Kontrolle von Schusswaffen und internationale Verträge über Fluggastdatensätze). Es hat den Anschein, als hielte die Kommission im Gegensatz zu Parlament und Rat eine einzige, kohärente Vision des künftigen Bereichs der Freiheit, der Sicherheit und des Rechts nicht länger für sinnvoll.
9. Am 2. April 2014 nahm das Europäische Parlament eine Entschließung zum Stockholmer Programm an.¹⁷ In dieser Entschließung wird unter anderem der Europäische Rat aufgefordert, einen „europäisches digitalen Habeas Corpus-Grundsatz“ bei Grundrechten umzusetzen und den Beitritt zur Europäischen Menschenrechtskonvention zu beschleunigen, wird das Parlament aufgefordert, in einer neuen Strategie der inneren Sicherheit ab 2014 bei der Bewertung und Festlegung der Maßnahmen für innere Sicherheit eine entscheidende Rolle zu spielen, und wird ein „zukunftsorientierter Ansatz in Bezug auf die Gestaltung und Optimierung der gemeinsamen Datennutzung im Bereich der Strafverfolgung in der EU bei gleichzeitiger Sicherstellung der Einhaltung der Grundrechte und eines hohen Maßes an Datenschutz“ gefordert. Generell forderte das Parlament eine „engere Zusammenarbeit und einen verbesserten Informationsaustausch zwischen den Organen der EU, ihren Einrichtungen und den Mitgliedstaaten [zur] Verbesserung der Gestaltung und der Umsetzung politischer Strategien“ und war der Ansicht, dass „die Verbesserung der Qualität der Rechtsvorschriften in der EU [...] gemeinsame Anstrengungen der Mitgliedstaaten und der europäischen Organe erforderlich macht“.

¹⁴ EUCO 217/13. Während sich frühere Mehrjahresprogramme stets über fünf Jahre erstreckten, die mehr oder weniger mit den Amtszeiten des Kollegiums der Kommissare und den Legislaturperioden des Europäischen Parlaments zusammenfielen, liegt der zeitliche Rahmen für die geplanten strategischen Leitlinien noch nicht fest. Der Rat hat die Möglichkeit einer Anpassung der neuen Leitlinien an den derzeitigen siebenjährigen Mehrjahresfinanzrahmen 2014-2020 erörtert.

¹⁵ KOM(2014) 144 endgültig.

¹⁶ KOM(2014) 154 endgültig.

¹⁷ Entschließung des Europäischen Parlaments vom 2. April 2014 zu der Halbzeitbilanz des Stockholmer Programms (2013/2024(INI)).

10. Der Rat hat in der Zwischenzeit eine Reihe von Aussprachen über die Zukunft des Bereichs Justiz und Inneres geführt, die auch Thema in den Beratungen des neu gewählten Europäischen Parlaments sein wird. Wie die Kommission tendiert auch der Rat eher zur Festlegung breiter politischer Prioritäten und weniger zu einer detaillierten Programmplanung wie in den vergangenen zehn Jahren, eher zur Konsolidierung oder Vereinfachung bestehender Maßnahmen als zu neuen Rechtsvorschriften und eher zu faktengestützten Ansätzen auf der Grundlage von Folgenabschätzungen.

3. DATENSCHUTZ UND DAS STOCKHOLMER PROGRAMM

Nach wie vor besteht dringender Bedarf an einem umfassenden und belastbaren Regelwerk

11. Seit der Verabschiedung des Stockholmer Programms hat die EU deutliche Schritte zur Stärkung der Grundrechte und hier vor allem des Rechts auf Privatsphäre und auf Datenschutz unternommen. Mit dem Inkrafttreten des Vertrags von Lissabon wurde die Charta rechtsverbindlich, und gemäß Artikel 16 AEUV hat die EU Datenschutzvorschriften für die Ausübung von Tätigkeiten zu erlassen, die in den Anwendungsbereich des Unionsrechts fallen. Besonders dringlich ist die Annahme eines neuen und umfassenden Datenschutzregelwerks. Die wichtigsten Meilensteine für den Datenschutz waren im Zeitraum der Umsetzung des Stockholmer Programms die Vorschläge der Kommission vom Januar 2012 zur Reform des Datenschutzrahmens und die legislative Entschließung des Europäischen Parlaments zu der Reform vom März 2014. Bedauerlicherweise sind im Rat keine großen Fortschritte zu verzeichnen gewesen, und der EDSB fordert alle Beteiligten auf, so bald wie möglich zu einer Einigung zu gelangen.
12. Der ehrgeizige Vorschlag, der das Kernstück des bestehenden Datenschutzrechts, die Richtlinie 95/46/EG, durch eine unmittelbar geltende Verordnung – die „allgemeine Datenschutzverordnung“ – ersetzen soll, hebt auf eine Stärkung der Rechte des Einzelnen, auf eine größere Rechenschaftspflicht der für die Verarbeitung Verantwortlichen, auf eine gestärkte nationale Aufsicht der Einhaltung der Vorschriften und mehr Rechtssicherheit für Unternehmen ab.
13. Die Richtlinie 95/46/EG gilt nicht für Tätigkeiten des Staates im Bereich des Strafrechts (Artikel 3 Absatz 2) und sieht für die Mitgliedstaaten die Möglichkeit vor, die Pflichten und Rechte zu beschränken, sofern dies unter anderem notwendig ist für „die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten“ (Artikel 13 Absatz 1). Die Verarbeitung von Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen kann erhebliche Auswirkungen auf das Leben einer Person haben. Das derzeitige Instrument, der Rahmenbeschluss 2008/977/JI des Rates, deckt jedoch nur die grenzüberschreitende Datenverarbeitung ab und lässt den Mitgliedstaaten einen großen Ermessensspielraum bezüglich der Anwendung der Grundsätze. Die vorgeschlagene Richtlinie, die an die Stelle des Rahmenbeschlusses 2008/977/JI treten soll, würde für die Verarbeitung im Inland gelten, ohne allerdings die verschiedenen bestehenden Vorschriften in Instrumenten der polizeilichen und justiziellen Zusammenarbeit zu berühren oder zu verbessern.

14. Daher hat der EDSB mit Bedauern festgestellt, dass die Kommission eine einzigartige Chance hat verstreichen lassen, ein einziges umfassendes Regelwerk mit einem hohen Maß an Datenschutz vorzuschlagen.¹⁸ Beharrt der Gesetzgeber auf einem eigenständigen Instrument für die polizeiliche und justizielle Zusammenarbeit, muss die vorgeschlagene Richtlinie ein Datenschutzniveau bieten, das dem der vorgeschlagenen Verordnung gleichwertig ist. Es gilt, offensichtliche Lücken zwischen den beiden Instrumenten zu schließen, so z. B. den Mangel an Klarheit bezüglich der Verantwortlichkeiten in Fällen, in denen mehrere Akteure an der Datenverarbeitung beteiligt sind und diese mehreren Zielen dient.

Erste zu bewertende Bemühungen

15. Im Bereich Inneres legte die Kommission im Dezember 2012 ein „Europäisches Modell für den Informationsaustausch“ als die im Stockholmer Programm versprochene Informationsmanagementstrategie vor.¹⁹ Dieses Dokument, das zu dem Schluss kam, dass weder neue Strafverfolgungsdatenbanken auf EU-Ebene noch neue EU-Instrumente für den Informationsaustausch erforderlich sind, war ein erster willkommener Schritt einer umfassenden Bewertung der Wirksamkeit der Verwendung von Daten bei der Kriminalitätsbekämpfung, die der EDSB seit langem gefordert hatte.
16. Alles in allem ergeben die Datenschutzstandards für Tätigkeiten im Bereich Justiz und Inneres allerdings nach wie vor nur einen Flickenteppich, der nach den Worten des Europäischen Parlaments „komplex und diffus ist, was eine ineffiziente Nutzung der verfügbaren Instrumente und eine unzureichende demokratische Kontrolle und Rechenschaftspflicht auf EU-Ebene nach sich zieht“.²⁰

Konkrete Maßnahmen

17. Auf die Notwendigkeit strenger und spezifischer Bedingungen für die Weitergabe personenbezogener Daten von privaten Parteien an Strafverfolgungsbehörden hat der EuGH in seinem Urteil zur Richtlinie über die Vorratsdatenspeicherung eindeutig hingewiesen.²¹ Wie aber beispielsweise an dem Abkommen mit den USA über das Programm zum Aufspüren der Finanzierung des Terrorismus deutlich wurde, besteht eine Tendenz, Strafverfolgungsbehörden Zugriff auf personenbezogene Daten im Besitz des privaten Sektors zu gewähren. Dies war einer der Hauptgründe für die Ablehnung des ersten Abkommens mit den Vereinigten Staaten durch das Europäische Parlament.²² Darüber hinaus besteht generell die Tendenz (siehe z. B. die Eurodac-Verordnung, die Vorschläge betreffend Fluggastdatensätze und das Paket „Intelligente Grenzen“),

¹⁸ Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket.

¹⁹ KOM(2012) 735 endgültig.

²⁰ Punkt 66, Entschließung 2013/2024(INI).

²¹ Vgl. weiter oben Fußnote 5.

²² Siehe Arbeitsunterlage der Kommissionsdienststellen SEK(2011) 438 endgültig.

Strafverfolgungsbehörden Zugriff auf personenbezogene Daten natürlicher Personen zu gewähren, die eigentlich für andere Zwecke erhoben wurden.²³

18. Bezüglich dieser Vorschläge haben wir wiederholt Bedenken vorgetragen. Der Widerstand gegen Initiativen in diesem Bereich ist Ausdruck der gestiegenen Sensibilität der Öffentlichkeit bei Maßnahmen, die möglicherweise in Grundrechte eingreifen (die Ablehnung des Handelsabkommens zur Bekämpfung von Produkt- und Markenpiraterie durch das Europäische Parlament ist ein ähnlich gelagerter bekannter Fall, der allerdings nicht dem Raum der Freiheit, der Sicherheit und des Rechts zuzuordnen ist), die infolge der Enthüllungen über die National Security Agency im Jahr 2013 noch zugenommen haben dürfte. Schon vor der Nichtigerklärung der Richtlinie über die Vorratsdatenspeicherung durch den EuGH hatten Mitglieder des Europäischen Parlaments die Richtlinie wiederholt kritisiert. Einzelstaatliche Gesetze über die Vorratsdatenspeicherung dürften aufgrund der vom Gerichtshof bemängelten fehlenden Verhältnismäßigkeit und unzureichenden Garantien nunmehr angefochten werden.

4. DER RAUM DER FREIHEIT, DER SICHERHEIT UND DES RECHTS UND DATENSCHUTZ: RISIKEN UND CHANCEN

Strategische Bewertung der Notwendigkeit der Erhebung und Verarbeitung personenbezogener Daten

19. Die Enthüllungen im vergangenen Jahr über Massenüberwachungsprogramme haben auf sehr dramatische und fühlbare Weise deutlich gemacht, dass es dringend geboten ist, sich mit den Interessen des Einzelnen zu befassen, nicht nur als Kunde von Online-Diensten, sondern als Bürger mit den Grundrechten auf Privatsphäre und Schutz personenbezogener Daten. Ein harmonisiertes und sachdienliches Datenschutzregelwerk ist Ausdruck sowohl der Kernwerte als auch der wirtschaftlichen Aufgabe der EU und sollte wie die Justizpolitik insgesamt als ein „Instrument zur Unterstützung des wirtschaftlichen Aufschwungs, des Wachstums und der Strukturreformen“ angesehen werden.²⁴ Wenn es darum geht, den Mehrwert eines EU-Konzepts für den Raum der Freiheit, der Sicherheit und des Rechts nachzuweisen, kann der Datenschutz eine Schlüsselrolle spielen.
20. Der EDSB hat die Kommission aufgefordert, eine Bewertung der Eingriffe in Grundrechte aufgrund des technologischen Wandels, der Entwicklungen bei IT-Großsystemen und der zunehmenden Verwendung von ursprünglich nicht für den Zweck der Verbrechensbekämpfung erhobenen Daten sowie der Frage vorzunehmen, inwieweit sich der derzeitige Trend einer verbreiteten, systematischen und proaktiven Überwachung nicht verdächtiger Personen als wirksam für die öffentliche Sicherheit erweist und für die Verbrechensbekämpfung tatsächlich von Nutzen ist.²⁵

²³ Siehe z. B. die Stellungnahme des EDSB vom 15. Dezember 2010 über die Einrichtung von „Eurodac“ für den Abgleich von Fingerabdruckdaten und die Stellungnahme des EDSB vom 18. Juli 2013 zu den Vorschlägen für eine Verordnung über ein Einreise-/Ausreiseregistersystem (EES) und eine Verordnung über ein Registrierungsprogramm für Reisende (RTP).

²⁴ KOM(2014) 144 endgültig, S. 3.

²⁵ Stellungnahme des Europäischen Datenschutzbeauftragten vom 29. April 2013 zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das europäische Modell für den Informationsaustausch“.

21. Eine ganze Reihe von Maßnahmen und vorgeschlagenen Maßnahmen, die die Verarbeitung personenbezogener Daten vorsehen, waren nicht erfolgreich, weil dem Recht auf Privatsphäre und Schutz personenbezogener Daten nicht ausreichend Raum geschenkt wurde, was unserer Auffassung nach wiederum darauf zurückzuführen ist, dass es keine strategische und systematische Bewertung des künftigen Bedarfs und der politischen Ziele gegeben hat. Dies sollte im Wege der Berücksichtigung von Datenschutzanliegen in allgemeinen Folgenabschätzungen geschehen, durch Prüfung der Frage, ob sich Ziele durch eine bessere Anwendung bestehender Maßnahmen oder mit weniger eingreifenden alternativen Maßnahmen erreichen lassen²⁶, und durch Verbesserung der Datenqualität und Stärkung der Rechte und Rechtsbehelfsmöglichkeiten betroffener Personen.
22. Die Kommission beabsichtigt eine Überprüfung und Aktualisierung der Strategie für ein integriertes Grenzmanagement mit der Möglichkeit „integrierter“ Systeme und Plattformen. Ferner plant sie eine gemeinsam von Parlament, Kommission und Mitgliedstaaten vorzunehmende Überarbeitung der Strategie der inneren Sicherheit.²⁷ Der Rat hat seinerseits die Frage erörtert, ob der Bedarf an einer „umfassenden Vernetzung von Informations-, Kommunikations- und Datensystemen“ erkundet werden soll. Dabei wird sich die Möglichkeit bieten, innenpolitische Maßnahmen einer Bewertung zu unterziehen, einschließlich Initiativen wie „Intelligente Grenzen“, über die schon seit Jahren diskutiert wird. Fester Bestandteil dieser Bewertung müssen die Auswirkungen auf den Datenschutz sein. In diesem Zusammenhang und im Lichte der Forderung des EP nach einem europäischen digitalen Habeas-Corpus-Grundsatz sollte die EU unter besonderer Berücksichtigung einschlägiger Urteile des EuGH Meinungen zur Massenüberwachung sammeln²⁸.

Verständnis der tatsächlichen Auswirkungen konkreter Maßnahmen auf die Bürger

23. Die Kommission räumt ein, dass auch weiterhin ein bürgerzentrierter Ansatz im Bereich Freiheit, Sicherheit und Recht erforderlich ist. In ihren Mitteilungen über die Zukunft des Bereichs Justiz und Inneres gibt die Kommission die Auffassung mehrerer Mitgliedstaaten wieder, der zufolge die EU bisherige Fortschritte konsolidieren und bestehende Maßnahmen überprüfen und bewerten sollte anstatt noch mehr Rechtsvorschriften um der Rechtsvorschriften willen zu erlassen.²⁹ Am sinnvollsten wäre ein bürgerzentrierter Ansatz, der den Interessen und Grundrechten der Bürger Rechnung trägt, vor allem in Anbetracht der großen politischen und rechtlichen Herausforderungen, vor denen die EU-Politik steht. Zu den obersten politischen Zielen sollte es immer gehören, Eingriffe in das Recht auf Privatsphäre so gering wie möglich zu halten und einen besseren Schutz personenbezogener Daten zu gewährleisten.

²⁶ Im Einklang mit dem Urteil des EuGH in *Schecke und Eifert*, Randnrn. 81 und 86.

²⁷ KOM(2014) 154 endgültig, S. 9.

²⁸ Entschließung des Europäischen Parlaments vom 12. März 2014 über das 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 (2013/2188(INI)), Punkte 131-133.

²⁹ KOM(2014) 144 endgültig, S. 5-8; KOM(2014) 154 endgültig, S. 13.

24. Wie jedoch ein vor kurzem veröffentlichter Bericht der Europäischen Agentur für Grundrechte über Rechtsbehelfe zeigt, fehlt es dem normalen Bürger an Informationen und steht er vor unerschwinglich hohen Kosten, wenn er einen Rechtsbehelf gegen unrechtmäßige Datenverarbeitung einlegen will.³⁰ Auch wenn die Kommission feststellt, dass „eine enge Zusammenarbeit zwischen den nationalen Behörden bzw. den Verwaltungsstellen für die Wirksamkeit bestimmter EU-Rechte besonders wichtig“ ist³¹, muss in den neuen strategischen Leitlinien praktischen Schritten oberste Priorität eingeräumt werden, mit denen Personen in die Lage versetzt werden, den Schutz ihrer personenbezogenen Daten durchzusetzen. Die stünde im Einklang mit dem Aufruf der Kommission, „ergänzende Initiativen“ mit dem Ziel in Betracht zu ziehen, das „Leben der Bürger zu erleichtern“.
25. Folgenabschätzungen und faktengestützte Bewertungen sollten sich mit den tatsächlichen Auswirkungen von Maßnahmen befassen, in deren Rahmen personenbezogene Daten verarbeitet werden, und die Zahl der betroffenen Personen erfassen, auf die Risiken des Missbrauchs und Garantien gegen den Missbrauch solcher Daten sowie auf die der jeweiligen betroffenen Person im Falle eines Missbrauchs zur Verfügung stehenden Rechtsbehelfe eingehen. Bei der Durchführung von Maßnahmen und operativen Tätigkeiten mit umfangreichen Verarbeitungen von Daten einschließlich der im Rahmen der EU-Politikzyklus zu schwerer und organisierter Kriminalität erfolgenden sollten ferner alle Fälle oder mutmaßlichen Fälle von Missbrauch berücksichtigt und sollte auf Ausbildungsbedarf eingegangen werden.³² Besondere Beachtung hat hier der Unabhängigkeit der nationalen Aufsichtsbehörde zu gelten, deren Bedeutung der EuGH in den letzten Jahren in mehreren Urteilen nachdrücklich unterstrichen hat³³, und der Frage, wie die Aufsicht koordiniert werden kann, wie es derzeit bei Eurodac, Zoll, VIS und SIS II der Fall ist.

Kodifizierung und Standardisierung: eine Möglichkeit, den Flickenteppich zu beseitigen

26. Mit Blick auf den Bereich Justiz spricht sich die Kommission für die Kodifizierung von existierenden Gesetzen, Vorgehensweisen und der Rechtsprechung in den Feldern Zivil- und Handelsrecht, Verbraucherrechte und Strafrecht mit dem Argument aus, dies würde zu Vereinfachung und besserem Verständnis führen, das gegenseitige Vertrauen stärken und Unstimmigkeiten sowie widersprüchliche Auslegungen von Vorschriften im Raum der Freiheit, der Sicherheit und des Rechts beseitigen.³⁴ Es bleibt jedoch unklar, welche Folgen eine solche Kodifizierung hätte. Der EDSB hat wiederholt für einen kohärenteren Datenschutzstandard in diesem Bereich und nicht für die derzeitige Palette von Normen plädiert, die der Rechtssicherheit für alle Betroffenen, also zuständige Behörden, Wirtschaft oder Bürger, entgegensteht. Eine etwaige Kodifizierung sollte sich auf alle Instrumente im Bereich Freiheit, Sicherheit und Recht erstrecken, die sich auf das Recht

³⁰ Agentur für Grundrechte, Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten, 2013.

³¹ KOM(2014) 144 endgültig, S. 7.

³² KOM(2014) 154 endgültig, S. 9.

³³ Urteile des Gerichtshofs (Große Kammer) vom 9. März 2010 - *Kommission gegen Deutschland* (Rechtssache C-518/07), vom 16. Oktober 2012 - *Kommission gegen Österreich* (Rechtssache C-614/10) und vom 8. April 2014 - *Kommission gegen Ungarn* (Rechtssache C-288/12).

³⁴ KOM(2014) 144 endgültig, S. 9.

auf Schutz personenbezogener Daten auswirken, sollte aber gleichzeitig ausreichend Spielraum bieten, damit berechtigten öffentlichen Interessen Genüge getan werden kann.

27. Im Bereich Inneres verweist die Kommission auf die Rolle des Schengener Informationssystems bei der Gewährleistung von Sicherheit und Freizügigkeit und auf die Notwendigkeit, den Schengener Visakodex zu überarbeiten und „die weltweite Implementierung des Visa-Informationssystems zum Abschluss zu bringen“. Die Kommission erwägt eine Evaluierung der Auswirkungen eines „stärker auf der Bewertung von Einzelpersonen statt [sic] von Staatsangehörigkeiten basierenden Systems“.³⁵ Vernünftig wäre ein ausgewogenerer Ansatz bei der Verarbeitung personenbezogener Daten wie in VIS und SIS II. An der Richtlinie 2006/24/EG hat der EuGH unter anderem kritisiert, sie verlange keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen sei, und einer Bedrohung der öffentlichen Sicherheit, und sie sei nicht beschränkt auf Personen, Zeiträume und Orte, bei denen die Verarbeitung personenbezogener Daten möglicherweise zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnte.³⁶
28. Ein Schritt in Richtung individueller Risikobewertungen würde vermutlich mit sich bringen, dass über bestimmte Personen Informationen aus verschiedenen Quellen gesammelt und ausgewertet werden. Abgesehen von dem impliziten Bedarf an Mechanismen für die Überwachung der Datenqualität müsste bei der vorgesehenen Evaluierung eines solchen Ansatzes große Aufmerksamkeit dem Abwägen der Eingriffe in die Privatsphäre dieser Menschen und in ihr Recht auf den Schutz personenbezogener Daten gewidmet werden.³⁷ Zentrale Bedeutung kommt klaren und genauen Vorschriften für einen solchen Politikwechsel zu, in denen die Verantwortlichkeiten von für die Verarbeitung Verantwortlichen vor allem für den Fall festgelegt werden sollte, dass die Erhebung von Visa-Daten an Unterauftragnehmer vergeben werden darf.

Zusammenarbeit mit dem privaten Sektor

29. Deutlich unterstrichen wird in der Mitteilung der Kommission die Rolle des privaten Sektors bei der Umsetzung der Ziele im Bereich Inneres. Hierzu gehören vielfältige Maßnahmen einschließlich des vorgeschlagenen EU-Rahmens für die Verarbeitung von Fluggastdatensätzen, die Frage des Zugangs und der Nutzung von Telekommunikationsdaten nach der Nichtigerklärung der Richtlinie 2006/24/EG, die „Intensivierung“ der Zusammenarbeit zur Bekämpfung der Cyberkriminalität mit Hilfe des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, das vorgeschlagene neue Paket zur Bekämpfung der Geldwäsche und die Zusammenarbeit zwischen Europol und dem privaten Sektor nach einer neuen Europol-Verordnung.

³⁵ KOM(2014) 154 endgültig, S. 6.

³⁶ *Digital Rights Ireland*, Randnr. 59.

³⁷ Zu den Risiken bei der Entwicklung von Profilen auf der Grundlage unbekannter und sich weiter entwickelnder Beurteilungskriterien siehe die Stellungnahme des EDSB vom 25. März 2011 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

30. Der Zugriff für Strafverfolgungsbehörden auf personenbezogene Daten, die für andere Zwecke erhoben wurden, ruft erhebliche Bedenken hervor. Er ist eine Ausnahme vom Grundsatz der Zweckbindung, und daher muss er die strengen Kriterien des Datenschutzrechts und von Artikel 7 und 8 der Charta erfüllen. Erforderlich ist hierfür, die politischen Ziele klar festzulegen und Verfahrensgenauigkeit sowie ausreichende Garantien gegen Missbrauch vorzusehen. Die für den Bürger entstehende Gefahr aufgrund einer engeren Zusammenarbeit zwischen privatem und öffentlichem Sektor in Fragen der Strafverfolgung bedeutet zusammen mit einem dualen Rahmen ein Minus an Rechenschaftspflicht und Transparenz. Noch deutlicher wird dies, wenn die Zusammenarbeit auf freiwilliger Grundlage stattfindet. Es muss klar sein, wer der für die Einhaltung der Vorschriften zuständige für die Verarbeitung Verantwortliche ist und welche Datenschutzvorschriften gelten. Für eine solche Zusammenarbeit muss eine explizitere Rechtsgrundlage vorhanden und ein eindeutig benannter und rechtmäßiger Zweck für die Datenverarbeitung gegeben sein.

Zusammenarbeit mit Drittstaaten

31. Sowohl Kommission als auch Rat messen dem Zusammenspiel mit Drittstaaten in Bereichen wie Cyberkriminalität und Menschenhandel großes Gewicht bei. Die Kommission plant eine Evaluierung der Wirksamkeit der bestehenden Vereinbarungen in Bezug auf den Austausch von Informationen der Strafverfolgungsorgane mit Drittstaaten.³⁸ Inzwischen arbeitet sie weiter an einer Rahmenvereinbarung zwischen der EU und den USA über Privatsphäre und Datenschutz und Rechtsschutzmechanismen für EU-Bürger und überarbeitet das Abkommen mit Kanada über die Bereitstellung von Fluggastdatensätzen.³⁹
32. Der EDSB unterstützt den angestrebten Abschluss von Abkommen, die einen klaren rechtlichen Rahmen für einen derartigen Austausch von Daten zwischen Strafverfolgungsbehörden abstecken; sie sind notwendig und bieten bessere Datenschutzgarantien. Verpflichtungen aufgrund einer internationalen Übereinkunft können jedoch nicht den Grundsatz beeinträchtigen, dass EU-Maßnahmen Grundrechte zu achten haben, die durch übermäßige Überwachungstätigkeiten nicht verletzt werden können.⁴⁰ Abkommen dürfen keine massiven Datenübermittlungen in einem Bereich – nämlich der Strafverfolgung – legitimieren, in dem die Auswirkungen auf den Einzelnen besonders schwerwiegend sind und in dem daher strenge und zuverlässige Sicherheiten und Garantien umso nötiger sind; sie müssen klare Bedingungen für Übermittlungen an andere Behörden oder Drittstaaten festlegen und durchsetzbare Rechte einschließlich Rechtsbehelfsmechanismen für betroffene Personen in der EU vorsehen. Werden Ausnahmen aus Gründen der nationalen Sicherheit in Anspruch genommen, sollten die Ausnahmen eng definiert und angemessene Garantien und Beschränkungen vereinbart werden.

³⁸ KOM(2014) 154 endgültig, S. 12.

³⁹ Siehe die Stellungnahme des EDSB vom 30. September 2013 zu den Vorschlägen für Beschlüsse des Rates betreffend den Abschluss und die Unterzeichnung des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen.

⁴⁰ Siehe Urteil des EuGH vom 3. September 2008, verbundene Rechtssachen C-402/05 P und C-415/05 P, *Kadi und Al Barakaat International Foundation gegen Rat und Kommission*; siehe ferner die Entschließung 2013/2188(INI) des Europäischen Parlaments, Punkt 132.

Empfehlungen zur Berücksichtigung von Erwägungen zu Privatsphäre und Datenschutz

33. Für uns ist von entscheidender Bedeutung, dass Erwägungen zu Privatsphäre und Datenschutz bei der Ausarbeitung aller neuen Maßnahmen und Rechtsvorschriften im Raum der Freiheit, der Sicherheit und des Rechts berücksichtigt werden. Folgende Vorgehensweisen wären in diesem Zusammenhang denkbar:

- Berücksichtigung von Datenschutzerwägungen in allgemeinen Folgenabschätzungen;
- Bewertung von alternativen, weniger eingreifenden Mitteln zum Erreichen politischer Ziele;⁴¹
- Verbesserung der Datenqualität und Stärkung der Rechte und Rechtsbehelfsmöglichkeiten betroffener Personen;
- Bewertung des Informationsaustauschs vor dem Hintergrund der politischen Ziele;
- Gewährleistung, dass internationale Abkommen mit Drittstaaten das Recht von Personen aus der EU auf Datenschutz achten.

5. HIN ZU EINEM NEUEN KONZEPT FÜR DIE ZUSAMMENARBEIT

34. In den kommenden Jahren werden die EU-Organen ein hochentwickeltes Instrumentarium für die politische Entscheidungsfindung benötigen, mit dem sichergestellt wird, dass alle Maßnahmen im Raum der Freiheit, der Sicherheit und des Rechts, die irgendwie in das Recht auf Privatsphäre und Datenschutz eingreifen, zu ihren Zielsetzungen in einem angemessenen Verhältnis stehen, präzise formuliert sind und umfassende Garantien gegen Missbrauch enthalten. Wir empfehlen, in den strategischen Leitlinien des Europäischen Rates auf dieses Instrumentarium zu verweisen. In unserem Strategiepapier „The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience“ (Der EDSB als Berater von EU-Organen in Fragen von Politik und Gesetzgebung, gestützt auf zehnjährige Erfahrungen)⁴² haben wir angekündigt, ein so genanntes „Policy Toolkit“ zu entwickeln, das auch allgemeine Hilfestellung für den Gesetzgeber beispielsweise in Form thematischer oder sektoraler Leitlinien enthalten soll. Dieses Toolkit soll den Organen dabei helfen, in voller Kenntnis der Auswirkungen neuer Vorschläge auf den Datenschutz Entscheidungen zu treffen, und besonders hilfreich könnte er in den Bereichen Freiheit, Sicherheit und Recht sein.

35. Wir sind nach wie vor bereit, gemeinsam mit den Organen an einer Strategie und praxisbezogenen Methodik zur Gewährleistung des Datenschutzes zu arbeiten, damit die EU legitime Ziele wirksamer und effizienter erreichen kann.⁴³ In sektorspezifischen Leitlinien könnten die praktischen Schritte zur Beurteilung der Legitimität des Zwecks und der Verhältnismäßigkeit und zur Festlegung von Mindestgarantien dargestellt werden. Zweck solcher Leitlinien wäre es, Personen, deren Daten verarbeitet werden,

⁴¹ Im Einklang mit dem Urteil des EuGH in *Schecke und Eifert*, Randnrn. 81 und 86.

⁴² Siehe Fußnote 11.

⁴³ Das Strategiepapier des EDSB enthält unter anderem das Angebot, mit den einzelnen Organen Vereinbarungen abzuschließen, um die Qualität der Gesetzgebung zu verbessern.

ausreichende Garantien gegen das Risiko des Missbrauchs und gegen unrechtmäßigen Zugriff und unrechtmäßige Verwendung zu geben.⁴⁴ Die Leitlinien sollten ferner die Qualität der Gesetzgebung auf allen Stufen verbessern helfen, auf denen ein verhältnismäßiger Eingriff in Grundrechte aus Gründen eines legitimen öffentlichen Interesses gerechtfertigt sein könnte. Rechnung getragen wird dabei der Entwicklung der Rechtsprechung zu den Kriterien für die Bewertung der Notwendigkeit und Verhältnismäßigkeit einer Maßnahme und natürlich ausreichenden Fortschritten in Richtung Annahme des überarbeiteten Datenschutzregelwerks.

6. SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

36. Insbesondere Mitgliedstaaten stellen immer wieder den Mehrwert eines Tätigwerdens der EU in den Bereichen Freiheit, Sicherheit und Recht in Frage. Der Nutzen liegt in einem einheitlichen Ansatz, beispielsweise durch den Entwurf verhältnismäßiger interoperabler Systeme, die sich gleichzeitig auch positiv auf Sicherheit und Datenschutz auswirken können. Die neuen strategischen Leitlinien bieten unserer Auffassung nach den Organen eine hervorragende Gelegenheit, Lehren aus den Erfahrungen zu ziehen und ein Instrumentarium zusammenzustellen, mit dem sich die oft unzureichenden Garantien für das Grundrecht auf Schutz personenbezogener Daten verbessern lassen.
37. Die EU muss beweisen, dass sie ihre Lektion aus den letzten fünf Jahren gelernt hat und keine Maßnahmen erlassen kann, die bei genauem Hinsehen einen Eingriff in Grundrechte darstellen und die Prüfung der Notwendigkeit und Verhältnismäßigkeit nicht bestehen. Wie die Kommission immer wieder ausgeführt hat, muss nun die Charta die Richtschnur für Politiken und Rechtsvorschriften der EU sein. Der EDSB ist bereit, bei diesem Prozess Hilfestellung zu leisten.
38. Die neuen Leitlinien des Europäischen Rates bieten der Union eine gute Möglichkeit zur Belegung ihrer Absicht, das Vertrauen in ihre Fähigkeit zum wirksamen Schutz von Personen wiederherzustellen. Daher schlagen wir dem Europäischen Rat vor, in den neuen Leitlinien ausdrücklich auf folgende Themen einzugehen:
 - a. die Verarbeitung der riesigen Mengen personenbezogener Daten, die in vielen Rechtsvorschriften und Politiken der EU im Bereich Freiheit, Sicherheit und Recht verlangt wird;
 - b. die Fragilität von Maßnahmen, die Grundrechte nicht achten, wie an der Richtlinie über die Vorratsdatenspeicherung deutlich wurde; diese Fragilität kann auch bei anderen laufenden Initiativen wie dem Paket „Intelligente Grenzen“ und verschiedenen Instrumenten zum Thema Fluggastdatensätze auftreten;
 - c. die Bedeutung einer möglichst baldigen Annahme eines starken und modernisierten Datenschutzregelwerks in der EU, der auch der Außenpolitik der EU als Richtschnur dienen sollte, und

⁴⁴ *Digital Rights Ireland*, Randnrn. 54, 60, 62, 65 und 67.

- d. das Erfordernis einer Berücksichtigung von Erwägungen zu Privatsphäre und Datenschutz bei der Ausarbeitung aller neuen Maßnahmen und Rechtsvorschriften im Raum der Freiheit, der Sicherheit und des Rechts.
39. Sichergestellt werden könnte eine Berücksichtigung von Erwägungen zu Privatsphäre und Datenschutz bei der Ausarbeitung aller neuen Maßnahmen und Rechtsvorschriften im Raum der Freiheit, der Sicherheit und des Rechts durch:
- Berücksichtigung von Datenschutzerwägungen in allgemeinen Folgenabschätzungen;
 - Bewertung von alternativen, weniger eingreifenden Mitteln zum Erreichen politischer Ziele;
 - Verbesserung der Datenqualität und Stärkung der Rechte und Rechtsbehelfsmöglichkeiten betroffener Personen;
 - Bewertung des Informationsaustauschs vor dem Hintergrund der politischen Ziele und
 - Gewährleistung, dass internationale Abkommen mit Drittstaaten das Recht von Personen aus der EU auf Datenschutz achten.

Brüssel, den 4. Juni 2014

(unterzeichnet)

Peter HUSTINX