Stellungnahme des Europäischen Datenschutzbeauftragten

zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“ und zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Über die Funktionsweise der Safe-Harbour-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen“

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 Datenverkehr[1],

gestützt auf die Verordnung (EG) des Rates 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 Datenverkehr[2], insbesondere auf Artikel 41 –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

I.1. Konsultation des EDSB

1. Am 27. November 2013 nahm die Kommission die Mitteilung der Kommission an das Europäische Parlament und den Rat „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“ an[3] („Mitteilung über die Wiederherstellung des Vertrauens“). Dieser Mitteilung beigefügt ist ein Bericht über

[1] ABl. L 281 vom 23.11.1995, S. 31, („Richtlinie 95/46/EG“).
[2] ABl. L 8 vom 12.1.2001, S. 1, („Verordnung (EG) Nr. 45/2001“).
[3] COM(2013) 846 final.

Postanschrift: Rue Wiertz 60 - B-1047 Brüssel
Dienststelle: Rue Montoyer 30 – B-1000 Brüssel
E-Mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

die Ergebnisse der EU-Ko-Vorsitzenden der Ad-hoc-Arbeitsgruppe EU-USA („Bericht“ und „Arbeitsgruppe“).

2. Am gleichen Tag nahm die Kommission eine Mitteilung der Kommission an das Europäische Parlament und den Rat „Über die Funktionsweise der Safe-Harbour-Regelung aus der Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen“ an[4] („Safe-Harbour-Mitteilung“).

3. Der EDSB begrüßt, dass er die Möglichkeit erhielt, vor der Annahme der genannten Dokumente der Kommission informelle Kommentare zukommen zu lassen. Diese Dokumente wurden von der Kommission nach den Enthüllungen über die Überwachungsprogramme US-amerikanischer Nachrichtendienste angenommen. In Anbetracht der Auswirkungen dieser Überwachungsprogramme auf das Recht natürlicher Personen auf Privatsphäre und den Schutz personenbezogener Daten hat der EDSB beschlossen, die vorliegende Initiativstellungnahme anzunehmen.

I.2. Ziel und Anwendungsbereich der Kommissionsdokumente

a) Mitteilung über die Wiederherstellung des Vertrauens und Bericht

4. Die Mitteilung macht Vorschläge für das weitere Vorgehen nach den Enthüllungen über umfassende Datenerhebungsprogramme der Geheimdienste der USA („die Programme“ oder „die enthüllten Programme“) und geht auf deren Auswirkungen auf das Vertrauen zwischen der EU und den USA ein. Sie geht nicht auf Enthüllungen über ähnliche Tätigkeiten und/oder die Zusammenarbeit von EU-Mitgliedstaaten oder anderen Drittstaaten und den USA ein.

5. Der Bericht enthält die Ergebnisse der EU-Ko-Vorsitzenden der Ad-hoc-Datenschutzarbeitsgruppe EU-USA, die nach der AStV-Sitzung vom 18. Juli 2013 eingesetzt wurde und den Auftrag hat, Fakten über die Programme und deren Auswirkungen auf die Grundrechte in der EU und auf personenbezogene Daten von EU-Bürgern zusammenzutragen. Er legt den einschlägigen Rechtsrahmen der USA dar[5], erläutert die Erhebung und Weiterverarbeitung der Daten[6] und schildert die bestehenden Mechanismen für Aufsicht und Rechtebehelfe.

6. In dem Bericht wird ein „zweiter Weg“ erwähnt, der ebenfalls auf der AStV-Sitzung am 18. Juli 2013 festgelegt wurde. Hierzu heißt es dort, dass im Rahmen dieses „zweiten Weges“ EU-Organe gegenüber den US-Behörden Fragen im Zusammenhang mit der mutmaßlichen Überwachung von Organen und diplomatischen Vertretungen der EU ansprechen können, während die Mitgliedstaaten mit den US-Behörden in bilateralen Gesprächen Fragen betreffend ihre nationale Sicherheit erörtern können.

[4] COM(2013) 847 final.

[5] Insbesondere die Verfassung in der Auslegung durch den Obersten Gerichtshof; Abschnitt 702 des *Foreign Intelligence Surveillance Act* (Gesetz über die Überwachung von Auslandsgeheimdiensten) von 1978 (FISA) (geändert durch den *2008 FISA Amendments Act*, 50 U.S.C. § 1881a); und Abschnitt 215 des *USA PATRIOT Act 2001* (der auch FISA änderte, 50 U.S.C. 1861) und *Executive Order 12333*.

[6] Auf der Grundlage von Informationen der USA in der Arbeitsgruppe und freigegebener Dokumente einschließlich Stellungnahmen des *Foreign Intelligence Surveillance Court* („FISC“) und öffentlich zugänglicher Dokumente wie der *Attorney General's Guidelines for Domestic FBI Operations*.

7. In dem Bericht heißt es ferner, dass diese Aufteilung eine gewisse Beschränkung der Diskussionen in der Arbeitsgruppe und der dort bereitgestellten Informationen bedeutete. Dem EDSB liegen keine Informationen über den „zweiten Weg“ oder die Einsetzung einer diesbezüglichen Parallelarbeitsgruppe vor. Die Kommission wird daher aufgefordert, den EDSB über die Ergebnisse des „zweiten Wegs“ zu unterrichten, insbesondere in Hinblick auf die mutmaßliche Überwachung von Organen und diplomatischen Vertretungen der EU.

b) Safe-Harbour-Mitteilung

8. In der Safe-Harbour-Mitteilung wird die Funktionsweise der Safe-Harbour-Regelung analysiert, werden Schwachstellen aufgezeigt und Verbesserungsmöglichkeiten vorgeschlagen. Sie bestätigt, dass zunehmend Daten zwischen der EU und den USA übermittelt werden und dass sich immer mehr Unternehmen zu den Safe-Harbour-Grundsätzen bekennen. Die Kommission beschreibt zunächst Struktur und Funktionsweise der Safe-Harbour-Regelung und unterstreicht dann die Notwendigkeit einer besseren Durchsetzung der Grundsätze der teilnehmenden Unternehmen und ihrer Subunternehmer. Gemäß der Mitteilung würde dies erfordern, dass die Safe-Harbour-Grundsätze wirksamer in die Datenschutzstrategien der beteiligten Unternehmen übernommen und der Öffentlichkeit zugänglich gemacht werden. Die FTC sollte sich zunehmend proaktiv für ihre Einhaltung einsetzen. Außerdem sollten sich die Datenschutzbehörden in der EU an Aufklärungskampagnen zum Thema Safe Harbour und hier vor allem zur Existenz der Europäischen Datenschutzkommission beteiligen. Die Kommission unterbreitet ferner Vorschläge für bessere alternative Streitbeilegungsmechanismen.

9. Im Hinblick auf den Zugang zu Daten, die im Rahmen der Safe-Harbour-Regelung übermittelt und von US-Behörden weiter verarbeitet werden, unterstreicht die Kommission, dass der Zugang auf das unbedingt erforderliche Maß beschränkt und verhältnismäßig sein sollte. Weiter verlangt sie, Einschränkungen des Schutzes des Privatsphäre aus Gründen der nationalen Sicherheit, des öffentlichen Interesses oder der Strafverfolgung sorgfältig überwacht werden sollten, damit dadurch der bestehende Schutz nicht gefährdet wird. Sie fordert teilnehmende Unternehmen auf, sich bezüglich dieser Einschränkungen und ihrer Auswirkungen auf die Vertraulichkeit der Kommunikation transparent zu zeigen und damit die Bürger zu sensibilisieren.

I.3. Gegenstand und Ziel dieser Stellungnahme

10. Gegenstand dieser Stellungnahme ist im Wesentlichen die Mitteilung über die Wiederherstellung des Vertrauens und, damit zusammenhängend, die Safe-Harbour-Mitteilung. Sie äußert sich folglich nicht direkt zu Enthüllungen betreffend EU-Mitgliedstaaten, in Zusammenarbeit mit den USA oder von sich aus, oder zu Beobachtungstätigkeiten anderer Drittländer als den USA.

11. Am Anfang der Stellungnahme stehen Anmerkungen zum allgemeinen Ansatz der Kommission in der Mitteilung über die Wiederherstellung des Vertrauens. Teil II analysiert kurz die Anwendbarkeit des geltenden rechtlichen Rahmens und deren Konsequenzen und enthält einige Anmerkungen zur Safe-Harbour-Mitteilung. Da

sich die Artikel 29-Datenschutzgruppe[7] derzeit mit dem geltenden EU-Regelwerk und dem internationalen Rechtsrahmen befasst, geht die Stellungnahme in diesem Teil nicht näher auf dieses Thema ein. Teil III befasst sich mit den Empfehlungen der Kommission für das künftige Vorgehen.

I.4. Anmerkungen zum Ansatz der Mitteilung über die Wiederherstellung des Vertrauens

12. Im Mittelpunkt der Mitteilung steht die Tatsache, dass das Vertrauen zwischen der EU und den USA als strategischen Partnern durch die Enthüllungen über die Programme beeinträchtigt wurde und wiederhergestellt werden muss. Dem stimmt der EDSB zu.

13. Allerdings berühren die Programme, deren Existenz in einigen Fällen durch den Bericht eindeutig bestätigt wird[8], nicht nur das Vertrauen, sondern auch gesetzliche Rechte, die im Primär- und Sekundärrecht der EU und des Europarates verankert sind, insbesondere das Recht auf Privatsphäre und auf Datenschutz. Sie zeigen auch, in welchem Umfang derzeit unter dem US-Rechtsrahmen[9], wie er vom Obersten Gerichtshof der USA ausgelegt wird[10], durch das Ausland tatsächlich Datenerhebung betrieben wird. Der Bericht bestätigt ferner, dass der US-Rahmen für EU-Bürger keine Garantien, keinen Schutz, keine Rechte, keine Kontrolle und keine Rechtsbehelfsmöglichkeiten vorsieht[11].

14. Wie die Kommission wiederholt unterstrichen hat, hängt das Vertrauen von Bürgern und Unternehmen in Kommunikation über das Internet von wirksamen Instrumenten für den technischen Schutz der Privatsphäre und hier vor allem von der Wahrung der Vertraulichkeit der Kommunikation ab. Dieses Bedürfnis hat auch die *US Review Group on Intelligence and Communications Technologies*[12] erkannt, die mehrere Empfehlungen für die Wiederherstellung des Vertrauens in Verschlüsselungswerkzeuge und kommerzielle Software und in die Funktionsweise von Schnellmechanismen für die Beseitigung von Softwareschwachstellen ausgearbeitet hat. Einige der anerkanntesten Sicherheitsexperten haben das geschwächte Vertrauen in diese Systeme als eine der schädlichsten Folgen der jüngsten Diskussionen über Fernmelde- und elektronische Aufklärungsaktionen

[7] Die nach der Richtlinie 95/46/EH eingesetzte Artikel 29-Datenschutzgruppe hat beratenden Status und ist unabhängig. Sie besteht aus Vertretern der nationalen Datenschutzbehörden in der EU, des EDSB und der Kommission.

[8] Siehe S. 5, 10 und 26 des Berichts, der, gestützt auf freigegebene Stellungnahmen des *Foreign Intelligence Surveillance Court* (US-Gericht zur Überwachung der Auslandsgeheimdienste) bestätigt, dass „US-Nachrichtendienste gemäß Abschnitt 702 auf weit reichende Erhebungsmethoden zurückgreifen können, wie die PRISM-Datenerhebung bei Internetprovidern oder die „vorgelagerte Erhebung" von Daten, die durch die USA übermittelt werden".

[9] Die USA haben bestätigt, dass es andere Rechtsgrundlagen für die mögliche Erhebung von Daten über Nicht-US-Bürger gibt, nannten jedoch keine Einzelheiten zu den rechtlichen Befugnissen und zu den Verfahren. Der Arbeitsgruppe wurden nicht alle einschlägigen Rechtsgrundlagen offengelegt (siehe S. 13 des Berichts).

[10] Siehe S. 4-12 des Berichts.

[11] Siehe S. 26-27 des Berichts.

[12] „Liberty and Security in a Changing World", Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, insbesondere Empfehlungen 25, 29 und 30. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

bezeichnet[13]. In Anbetracht der Bedeutung einer wirksamen Sicherheit im Internet für Europa sollte auf Initiative der Kommission auf EU-Ebene eine Antwort auf diese technische und politische Herausforderung formuliert werden.

15. In Abschnitt 3 der Mitteilung befasst sich die Kommission mit den künftigen Maßnahmen, mit denen das Vertrauen in Datenübermittlungen zwischen der EU und den USA wiederhergestellt werden soll. Der EDSB begrüßt diesen Abschnitt, in dessen Mittelpunkt die Verbesserung des bestehenden rechtlichen Rahmens steht, in dem aber auch neue Instrumente vorgeschlagen werden. Die Kommission geht allerdings nicht darauf ein, inwieweit die anzuwendenden Instrumente der Mitgliedstaaten, der EU und des Europarates von den Programmen berührt wurden. Nach Auffassung des EDSB hätten den Auswirkungen auf bestehende Rechtsinstrumente in der Mitteilung mehr Raum gewidmet werden müssen.

II. ANMERKUNGEN ZUM GELTENDEN RECHTSRAHMEN

II.1. Datenschutzregelwerke der EU und des Europarates

16. Das Recht auf Privatsphäre und auf Datenschutz ist im Primärrecht in Artikel 8 des Übereinkommens des Europarates zum Schutz der Menschenrechte und der Grundfreiheiten („EMRK"), in Artikel 7 und 8 der Charta der Grundrechte der EU („Charta") und in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union („AEUV") verankert. Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte („IPBPR"), der auch von den USA ratifiziert wurde, besagt, dass niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben ausgesetzt werden darf. Das Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten enthält genauere Vorschriften für den Datenschutz.

17. Im Sekundärrecht ist die Ausübung dieser Rechte geregelt in der Richtlinie 95/46/EG, im Rahmenbeschluss 2008/977/JI des Rates[14], in der Verordnung (EG) Nr. 45/2001 und in der Richtlinie 2002/58/EG[15], in der Auslegung durch den Gerichtshof der Europäischen Union. Hier sowie in Artikel 8 Absatz 2 EMRK und in Artikel 52 Absatz 1 der Charta sind die Kriterien und Bedingungen für eine Einschränkung ihrer Ausübung festgelegt.

18. Die vorstehend genannten Bestimmungen des EU-Rechts gelten nicht für die nationale Sicherheit von EU-Mitgliedstaaten, da gemäß Artikel 4 Absatz 2 des Vertrags über die Europäische Union („EUV") diese eine „grundlegende Funktion des Staates" der Mitgliedstaaten ist, die weiterhin in „ihre alleinige Verantwortung" fällt und daher auf einzelstaatlicher Ebene geregelt ist.

---

[13] B Schneier, C Soghoian im Bericht vom 6. September 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; B. Preneel: ISSE 2013 Schlussvortrag: „The Cryptographic Year in Review" http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

[14] 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. ABl. L 350 vom 30.12.2008, S. 6.

[15] 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). ABl. L 201 vom 31.7.2002, S. 37.

II.1.1. Geltungsbereich von Ausnahmen betreffend die nationale Sicherheit

a) Nationale Sicherheit als Faktor, der den Anwendungsbereich von EU-Instrumenten einschränkt

19. In der Mitteilung heißt es: „Die EU kann zwar im Rahmen ihrer Zuständigkeiten Maßnahmen ergreifen, um insbesondere die Einhaltung der EU-Rechtsvorschriften zu gewährleisten, die Wahrung der nationalen Sicherheit obliegt jedoch ausschließlich den Mitgliedstaaten“[16]. Der EDSB begrüßt diese Aussage betreffend die Zuständigkeit der EU, die Einhaltung der EU-Rechtsvorschriften zu gewährleisten. Der EDSB weist aber auch darauf hin, dass die nationale Sicherheit von Drittländern keine grundlegende Funktion oder alleinige Verantwortung von EU-Mitgliedstaaten ist und damit nicht unter diese Ausnahme fällt.

20. Der Ausschluss der nationalen Sicherheit von Mitgliedstaaten aus dem Anwendungsbereich des EU-Rechts bedeutet auf keinen Fall, dass die nationale Sicherheit ein unregulierter Bereich bleibt, insbesondere im Hinblick auf den Schutz von Grundrechten, denn die oben erwähnten Instrumente des Europarates[17] und innerstaatliches Recht finden in den meisten Fällen Anwendung auf diesen Bereich[18].

21. Selbst in Fällen, in denen das EU-Recht keine Anwendung findet, gilt doch die Europäische Menschenrechtskonvention und das Übereinkommen Nr. 108 für viele der fraglichen Verarbeitungen personenbezogener Daten, da ihre allgemeine Anwendung auf die meisten ihrer Vertragsparteien[19] nicht die nationale Sicherheit insgesamt ausnimmt[20]. Diese Instrumente enthalten auch die positive Verpflichtung für ihre Vertragsparteien, innerhalb ihres Zuständigkeitsbereichs jedermann das Recht auf Privatsphäre und Datenschutz zu gewährleisten[21] und innerstaatliche Rechtsvorschriften zur Verwirklichung der Datenschutzgrundsätze zu erlassen[22].

b) Einschränkung von in Instrumenten der EU und des Europarates verankerten Rechten durch die nationale Sicherheit

22. Finden die oben erwähnten Instrumente der EU und des Europarates Anwendung, kann das Recht auf Privatsphäre und auf Datenschutz bei Bedarf unter anderem aus Gründen der nationalen Sicherheit oder der Sicherheit des Staates eingeschränkt werden[23]. Solche Einschränkungen sind jedoch restriktiv auszulegen[24], und eine

[16] Siehe S. 4 der Mitteilung.
[17] Nur eine Minderheit der Vertragsparteien des Übereinkommens Nr. 108 hat eine Erklärung gemäß Artikel 3 Absatz 2 Buchstabe a abgegeben, die besagt, dass das Übereinkommen Nr. 108 nicht gilt für „automatisierte Sätze personenbezogener Daten“ im Zusammenhang mit „Sicherheit des Staats“ oder „Staatsgeheimnissen“.
[18] Siehe z. B. die Entscheidung des Bundesverfassungsgerichts in Sachen Rasterfahndung (BVerfG 1 BvR 518/02 vom 4.4.2006).
[19] Siehe Fußnote 17.
[20] Wie für EU-Instrumente gilt auch für Instrumente des Europarates, dass sie Einschränkungen bestimmter Rechte vorsehen, beispielsweise aus Gründen der nationalen Sicherheit. Solche Einschränkungen sind allerdings restriktiv auszulegen (siehe z. B. EGMR, *Klass und andere / Deutschland*, Urteil vom 6. September 1978, Reihe A Nr. 28).
[21] Siehe Artikel 1 und 8 EMRK.
[22] Siehe Artikel 4 Absatz 1 des Übereinkommens Nr. 108.
[23] Siehe z. B. Artikel 8 Absatz 2 EMRK, Artikel 9 Absatz 2 Buchstabe a und Artikel 13 Absatz 1 Buchstabe a der Richtlinie 95/46/EG.

Einschränkung der in diesen Instrumenten verankerten Rechte ist nur zulässig, wenn sie in einem vorhersehbaren und zugänglichen[25] Gesetz[26] vorgesehen ist, und nur, wenn sie in einer demokratischen Gesellschaft erforderlich ist[27].

23. Die in den genannten Instrumenten geregelten Ausnahmen aus Gründen der nationalen Sicherheit rechtfertigen daher keinesfalls massive Einschränkungen von Grundrechten wie die in den Programmen aus Gründen vorgesehenen, die weit über die nationale Sicherheit hinausgehen können und mehrheitlich mit den Interessen eines Drittlandes zu tun haben[28] und für die Wahrung der nationalen Sicherheit nicht zwingend erforderlich sind[29].

II.1.2. Durchsetzbarkeit der Regelwerke von EU und Europarat

a) Durchsetzbarkeit bei für die Verarbeitung Verantwortlichen

24. Einzelstaatliche Vorschriften zur Umsetzung der Richtlinie 95/46/EG sind auf Verarbeitungen im Rahmen der Tätigkeiten einer Niederlassung von für die Verarbeitung Verantwortlichen in der EU anzuwenden[30]. Sie gelten auch dann, wenn ein nicht in der EU niedergelassener für die Verarbeitung Verantwortlicher an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht eines Mitgliedstaats gemäß den internationalen Recht Anwendung findet, oder wenn der für die Verarbeitung Verantwortliche Ausrüstung in der EU verwendet[31]. In derartigen Fällen dürfen EU-Datenschutzbehörden also ihre innerstaatlichen Datenschutzvorschriften unmittelbar gegenüber Organisationen durchsetzen, die unter Verstoß gegen innerstaatliches Datenschutzrecht Regierungen von Drittländern Zugang zu personenbezogenen Daten verschaffen oder an sie Daten weitergeben.

25. Nachdem auch die Verordnung (EG) Nr. 45/2001 anzuwenden ist, hat der EDSB mit den Organen und Einrichtungen der EU Gespräche über Risiken für die Vertraulichkeit der Kommunikation und die Sicherheit der Verarbeitung sowie über die Annahme angemessener und wirksamer technischer Sicherheitsvorkehrungen aufgenommen.

---

[24] EGMR, *Klass und andere*, bereits zitiert, Randnr. 42.
[25] EGMR, *Rotaru / Rumänien*, Urteil vom 4. Mai 2000, Beschwerde Nr. 28341/95, Randnr. 48.
[26] Siehe Artikel 52 Absatz 1 der Charta.
[27] a.a.O.
[28] Gemäß der FISA – Definition dieses Begriffs könnte „*foreign intelligence*“ (Erkenntnisse aus der Tätigkeit von Auslandsgeheimdiensten) Informationen über die politische Tätigkeit von Personen oder Gruppen und die Tätigkeit von Regierungsstellen umfassen, sofern diese für die Außenpolitik der USA von Interesse sein könnten. Die EU-Vertreter in der Arbeitsgruppe baten um nähere Erläuterungen um Anwendungsbereich von „*foreign intelligence*“, die die USA jedoch mit dem Argument ablehnten, solche Erläuterungen würden spezifische operative Aspekte der Programme offenlegen. Siehe S. 5-7 des Berichts.
[29] Gemäß Abschnitt 702 des FISA gelten Daten über Nicht-US-Bürger als „*foreign intelligence*“, sobald sie mit den angestrebten Zielen *in Verbindung stehen*. Daten von US-Bürgern müssen hingegen als für das Erreichen der angestrebten Ziele *erforderlich* gelten, damit sie als „*foreign intelligence*“ angesehen werden. Siehe S. 26 des Berichts.
[30] Siehe Artikel 4 Absatz 1 Buchstabe a der Richtlinie 95/46/EG.
[31] Siehe Artikel 4 Absatz 1 Buchstabe b und c der Richtlinie 95/46/EG und deren Auslegung durch die Artikel 20-Datenschutzgruppe in deren Stellungnahme 8/2010 zum anwendbaren Recht (WP 179), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_de.htm.

b) Durchsetzbarkeit bei Vertragsparteien der EMRK

26. Artikel 1 und 8 EMRK schaffen für die Vertragsparteien des Übereinkommens eine positive Verpflichtung, das Recht auf Privatsphäre und auf Datenschutz zu schützen. Die Programme hatten zur Folge, dass dieser Verpflichtung nicht nachgekommen wurde. Das Übereinkommen Nr. 108, das auf Datenverarbeitungen durch den öffentlichen und den privaten Sektor in den Vertragsstaaten dieses Übereinkommens Anwendung findet, wurde in dem Zusammenhang ebenfalls nicht eingehalten.

27. EU-Mitgliedstaaten sowie alle anderen Vertragsparteien der EMRK können vor dem Europäischen Gerichtshof für Menschenrechte („EGMR") wegen Nichterfüllung ihrer Verpflichtung verklagt werden, „allen ihrer Hoheitsgewalt unterstehenden Personen die in dem Übereinkommen bestimmten Rechte und Freiheiten zu sichern"[32], insbesondere das Recht auf Achtung des Privatlebens[33]. Am 4. September 2013 wurde von *Big Brother Watch and Others* eine Beschwerde gegen das Vereinigte Königreich eingelegt[34].

II.2. Instrumente zur Regelung von Übermittlungen

a) Instrumente zur Regelung von Übermittlungen aus der EU in die USA innerhalb des privaten Sektors

28. Der Austausch personenbezogener Daten zwischen Privatunternehmen und Organisationen in der EU und in den USA erfolgt auf der Grundlage mehrerer Instrumente, die gestützt auf Artikel 25 und 26 der Richtlinie 95/46/EG angenommen wurden: Entscheidung der Kommission 2000/520/EG („Safe-Harbour-Entscheidung"), Entscheidungen der Kommission 2001/497/EG, 2004/915/EG und 2010/87/EU („Standardvertragsklauseln") und eine Reihe von Dokumenten der Artikel 29-Datenschutzgruppe zu verbindlichen unternehmensinternen Datenschutzvorschriften (*Binding Corporate Rules*) („BCR").

29. Einige dieser Instrumente (Safe Harbour und Standardvertragsklauseln) erlauben ein Abweichen von ihren Grundsätzen, sofern dies in einer demokratischen Gesellschaft erforderlich ist, z. B. aus Gründen der nationalen Sicherheit. In einigen Fällen (Safe Harbour, Standardvertragsklauseln und verbindliche unternehmensinterne Datenschutzvorschriften) verlangen sie eine Unterrichtung des aus der EU Übermittelnden oder der zuständigen EU-Datenschutzbehörde, wenn innerstaatliche Vorschriften im Empfängerland im Widerspruch zu in diesen Instrumenten verankerten Grundsätzen stehen.

30. Die Programme gehen allerdings über das erforderliche Maß hinaus, zumindest bei Daten von Nicht-US-Bürgern[35]. Diese Instrumente wurden auf jeden Fall nicht als Schutz gegen massive Weiterübermittlungen an die Regierung der empfangenden Organisation oder gegen den Zugang durch diese Regierung entworfen. Der EDSB empfiehlt daher Verbesserungen an diesen Instrumenten, insbesondere an

[32] Siehe Artikel 1 EMRK.
[33] Siehe Artikel 8 EMRK.
[34] *Big Brother Watch and Others / Vereinigtes Königreich*, Beschwerde Nr. 58170/13, abrufbar unter http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713, zuletzt abgerufen am 17.02.2014.
[35] Siehe Fußnote 29.

Safe Harbour, ein Punkt, der sowohl in der Mitteilung über die Wiederherstellung des Vertrauens als auch, noch intensiver, in der Safe-Harbour-Mitteilung erörtert wurde.

b) Umsetzung der Safe-Harbour-Regelung

31. Der EDSB begrüßt die Analysen und Empfehlungen der Kommission zur Umsetzung von Safe Harbour. In der Safe Harbour-Mitteilung heißt es, die Kommission habe Schwachstellen wie mangelnde Transparenz und unzureichende Durchsetzung festgestellt. Außerdem hielten sich einige selbstzertifizierte Safe Harbour-Unternehmen in der Praxis nicht an dessen Grundsätze, was sich unter anderem nachteilig auf die Grundrechte der EU-Bürger auswirke.

32. Ein Thema der Safe-Harbour-Mitteilung ist der „Zugriff auf im Rahmen der Safe-Harbour-Regelung übermittelten Daten". In der Mitteilung über die Wiederherstellung des Vertrauens wird die Frage erörtert, ob die umfassende Erfassung und Verarbeitung personenbezogener Informationen im Rahmen der Programme den Anforderungen der Safe-Harbour-Regelung an Notwendigkeit und Verhältnismäßigkeit entspricht. Die Kommission befindet, dass das System des sicheren Hafens „als Kanal für die Übertragung personenbezogener Daten von EU-Bürgern von der EU in die USA durch Unternehmen dient, die zur Freigabe von Daten an US-Geheimdienste aufgefordert werden".

33. In diesem Zusammenhang begrüßt der EDSB folgende bekräftigende Aussage der Kommission: „Grundrechtsbeschränkungen sind nur dann gültig, wenn sie eng ausgelegt werden, in einem der Öffentlichkeit zugänglichen Gesetz niedergelegt sind und in einer demokratischen Gesellschaft angemessen und notwendig sind"[36]. Jede Einschränkung von Datenschutzvorschriften aus Gründen der nationalen Sicherheit sollte diese Bedingungen erfüllen. Dieses Erfordernis der „Notwendigkeit" wird bereits in der Safe-Harbour-Entscheidung[37] erwähnt, wo es heißt: „Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss".

34. Der EDSB bedauert allerdings die Schlussfolgerung der Kommission: „Der breite Zugriff der US-Behörden auf Daten, die von selbstzertifizierten Safe-Harbour-Unternehmen verarbeitet werden, gefährdet die Vertraulichkeit der elektronischen Kommunikation", und dass sie nicht darauf eingeht, dass ein solcher Zugriff über die in den Safe-Harbour-Grundsätzen gezogenen Grenzen hinausgeht. Nach Auffassung des EDSB belegen sowohl der Umfang der Programme als auch die Tatsache, dass nach US-Recht das Erfordernis der „Notwendigkeit" nur für Daten von US-Bürgern gilt[38], dass die Programme im Hinblick auf Nicht-US-Bürger die Bedingung der Notwendigkeit nicht erfüllen[39].

[36] Siehe S. 17, erster Absatz, der Safe Harbour-Mitteilung.
[37] Siehe Anhang I, Grundsätze des „Sicheren Hafens" zum Datenschutz, Absatz 4.
[38] Siehe Fußnote 29.
[39] Siehe auch das Urteil des EuGH in der Rechtssache Huber, C-524/06.

c) Instrumente zur Regelung von Übermittlungen von der EU an die USA für Strafverfolgungszwecke

35. Neben den bereits erwähnten Instrumenten gibt es eine Reihe von Abkommen, die den Austausch personenbezogener Daten zwischen der EU und den USA für Strafverfolgungszwecke einschließlich Verhinderung und Bekämpfung von Terrorismus regeln:
- das Rechtshilfeabkommen (*Mutual Legal Assistance Agreement* („MLAA"))[40],
- das Abkommen über die Verwendung und Übermittlung von Fluggastdatensätzen (*Passenger Name Records*) („PNR-Abkommen")[41],
- das Abkommen über die Verarbeitung von Zahlungsverkehrsdaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (*Terrorist Financing Tracking Program*) („TFTP-Abkommen")[42] und
- das Abkommen zwischen Europol und den USA[43].

36. Ein Zugriff durch US-Behörden auf Daten, die nach EU-Recht verarbeitet wurden, sollte ausschließlich unter diesen Abkommen stattfinden.

37. In den Enthüllungen über die Programme wird behauptet, es habe möglicherweise Verstöße gegen das PNR-Abkommen und das TFTP-Abkommen gegeben. Nach Angaben der Kommission bleiben diese Behauptungen unbelegt[44]. In Anbetracht der jüngsten Entwicklungen sollte hier allerdings, insbesondere im Hinblick auf TFTP, unter Berücksichtigung der von der Gemeinsamen Kontrollinstanz von Europol geäußerten Bedenken[45] und der gemeinsamen Untersuchung der niederländischen und der belgischen Datenschutzbehörde[46] etwas vorsichtiger geurteilt werden.

38. Im Zusammenhang mit dem Informationsaustausch für Strafverfolgungszwecke behauptet die Mitteilung, das PNR-Abkommen und das TFTP-Abkommen sorgten für „ein hohes Schutzniveau bei den personenbezogenen Daten". Wie wiederholt

[40] Beschluss 2009/820/GASP des Rates vom 23. Oktober 2009 über den Abschluss im Namen der Europäischen Union des Abkommens über Auslieferung zwischen der Europäischen Union und den Vereinigten Staaten von Amerika und des Abkommens über Rechtshilfe zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, ABl. L 291 vom 7.11.2009, S. 40.

[41] Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security (Beschluss 2012/472/EU des Rates vom 26. April 2012, ABl. L 215 vom 11.8.2012, S. 4).

[42] Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (Beschluss des Rates vom 13. Juli 2010, ABl. L 195 vom 27.7.2010, S. 3).

[43] Abkommen zwischen den Vereinigten Staaten von Amerika und dem Europäischen Polizeiamt vom 6. Dezember 2001 und Ergänzendes Abkommen zwischen dem Europäischen Polizeiamt und den Vereinigten Staaten von Amerika über den Austausch personenbezogener Daten und zugehöriger Informationen vom 20. Dezember 2002.

[44] In der Mitteilung heißt es, dass weder die gemeinsame Überprüfung der Anwendung des PNR-Abkommens noch die von der Kommission aufgenommenen offiziellen Konsultationen zum TFTP-Abkommen „Hinweise auf Verletzungen dieser Abkommen erkennen ließen", und dass die USA schriftlich zugesichert haben, es sei keine direkte Datensammlung erfolgt, mit der gegen das TFTP-Abkommen verstoßen worden wäre.

[45] Bericht der Gemeinsamen Kontrollinstanz vom 18. März 2013 über die Anwendung des TFTP-Abkommens.

[46] Gemeinsame Presseerklärung der belgischen und niederländischen Datenschutzbehörde vom 14. November 2013.

dargelegt[47], ist das durch diese Abkommen gebotene Datenschutzniveau durchaus fragwürdig, weshalb eine solche Aussage nicht vorbehaltlos erfolgen darf[48].

39. Die Behauptungen, denen zufolge möglicherweise gegen das PNR-Abkommen und das TFTP-Abkommen verstoßen wurde, werden zwar nicht belegt, doch gibt es auch keinen Beweis für etwaige Untersuchungen in dieser Sache. Der EDSB behält sich vor, gesondert auf den gemeinsamen Überprüfungsbericht zu den US-PNR, die TFTP-Mitteilung und den gemeinsamen TFTP-Überprüfungsbericht einzugehen.

III. SPEZIFISCHE ANMERKUNGEN ZUM WEITEREN VORGEHEN

III.1. Reibungslose Annahme der EU-Datenschutzreform

40. Wie die Kommission ist auch der EDSB der Auffassung, dass in diesem Zusammenhang die Vorschläge für ein neues Datenschutzregelwerk („Vorschläge“)[49] eine wichtige Rolle spielen. In der Mitteilung werden fünf Elemente der Vorschläge besonders hervorgehoben: die Erweiterung des räumlichen Anwendungsbereichs, die Klarstellung der Voraussetzungen für Übermittlungen, die Harmonisierung und Stärkung der Durchsetzungsbefugnisse von EU-Datenschutzbehörden, die Aufnahme eindeutiger Bestimmungen zu den Verpflichtungen und zur Haftung von Auftragsverarbeitern und die Festlegung „umfassender Bestimmungen“ für den Schutz personenbezogener Daten im Bereich der Strafverfolgung.[50]

41. In diesem Zusammenhang weist der EDSB auf zwei weitere Punkte hin, die von den Mitgesetzgebern diskutiert werden: i) die Behandlung der Verarbeitung für Strafverfolgungszwecke von personenbezogenen Daten, die ursprünglich für kommerzielle Zwecke erhoben wurden, und ii) die Behandlung internationaler Normenkollisionen.

---

[47] Siehe folgende Stellungnahmen des EDSB: Stellungnahme vom 30. September 2013 zu den Vorschlägen für Beschlüsse des Rates über den Abschluss und die Unterzeichnung des Abkommens zwischen Kanada und der Europäischen Union über die Verwendung von Passagierdatensätzen; Stellungnahme vom 9. Dezember 2011 zu dem Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security; Stellungnahme vom 15. Juli 2011 zu dem Vorschlag für einen Beschluss des Rates über den Abschluss eines Abkommens zwischen der Europäischen Union und Australien über die Verwendung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an die australische Zoll- und Grenzschutzbehörde; Stellungnahme vom 19. Oktober 2010 zum sektorübergreifenden Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer; Stellungnahme vom 15. Juni 2005 zu dem Vorschlag für einen Beschluss des Rates über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und der Regierung Kanadas über die Verarbeitung von erweiterten Fluggastdaten (Advance Passenger Information (API)) und Fluggastdatensätzen (Passenger Name Record (PNR)); alle abrufbar unter www.edps.europa.eu.

[48] Siehe auch die Stellungnahmen der Artikel 29-Datenschutzgruppe zu PNR-Abkommen zwischen der EU und Drittländern, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[49] Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (KOM(2012)11) endgültig und Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (KOM(2012)10 endgültig).

[50] Siehe S. 5-6 der Mitteilung über die Wiederherstellung des Vertrauens.

42. Der erste dieser beiden Punkte bezieht sich auf die Tatsache, dass trotz der Möglichkeiten, die die neue Rechtsgrundlage Artikel 16 AEUV bietet, das Datenschutzpaket nicht aus einem einzigen, umfassenden Vorschlag, sondern aus zwei Vorschlägen mit unterschiedlichem sachlichem Geltungsbereich besteht. Hieraus könnte Rechtsunsicherheit in Fällen entstehen, in denen personenbezogene Daten, die ursprünglich der vorgeschlagenen Datenschutzverordnung unterliegen, in der Folge für Zwecke und durch Behörden verarbeitet werden, die der vorgeschlagenen Datenschutzrichtlinie unterliegen. Auf dieses Problem hatte die Kommission bereits in der Folgenabschätzung[51] hingewiesen, doch war es in den Vorschlägen nicht gelöst worden. Der EDSB empfiehlt den Mitgesetzgebern, dieses Versäumnis zu korrigieren und diese Fälle zu regeln.

43. Bezüglich internationaler Normenkollisionen sei darauf hingewiesen, dass alle Verarbeitungstätigkeiten, die in den Anwendungsbereich des Datenschutzpakets fallen, auch damit im Einklang stehen sollten, sofern nicht ein verbindliches internationales Abkommen, das angemessene Datenschutzgarantien bietet, anderes bestimmt, oder sofern nicht eine Justiz- oder Datenschutzbehörde eine Befreiung gewährt hat.

44. Der EDSB stimmt der abschließenden Bemerkung in der Mitteilung zu, der zufolge die Ereignisse der jüngeren Vergangenheit „ein Weckruf" für die EU und ihre Mitgliedstaaten sind, der sie daran erinnert, „die Reform der EU-Datenschutzvorschriften zügig und zielgerichtet voranzubringen".

III.2. Stärkung des Safe-Harbour-Systems

45. In der Mitteilung zur Wiederherstellung des Vertrauens schlägt die Kommission eine Stärkung des Safe-Harbour-Systems vor. Der EDSB begrüßt diesen Vorschlag, hätte jedoch eine positivere Formulierung bevorzugt. Wie bereits ausgeführt, unterstreicht der EDSB ferner die Notwendigkeit einer angemessenen rechtlichen Schlussfolgerung bezüglich der unzureichenden Wahrung der Safe-Harbour-Grundsätze.

46. So sollte insbesondere die Stärkung des Systems das *Ergebnis* der Überprüfung seiner Funktionsweise sein, und nicht umgekehrt. Zwar werden in der Mitteilung zur Wiederherstellung des Vertrauens mehrere Gründe für die Beibehaltung des Systems angeführt, doch sollte die Entscheidung letztendlich davon abhängen, wie die Empfehlungen des Berichts wirksam umgesetzt werden. Im Falle eines Scheiterns könnte immer noch die Aussetzung oder Aufhebung der Regelung ins Auge gefasst werden.

47. Es sind verschiedene Szenarien denkbar, einschließlich möglicher Maßnahmen in Abhängigkeit vom Ergebnis der Überprüfung. In solchen Szenarien sollte gründlich die mögliche Anwendung von Artikel 3 und/oder Artikel 4 der Safe-Harbour-Entscheidung analysiert werden und sollte erläutert werden, wann und unter welchen Bedingungen eine Aussetzung eine Option wäre, wann Artikel 4 die Grundlage für eine bessere Definition der Safe-Harbour-Grundsätze wäre, und vor allem, welchen

[51] Siehe Anhang III, S. 4 der Folgenabschätzung zu den Vorschlägen (SEC(2012) 72 final).

genauen Geltungsbereich die Ausnahme aus Gründen der nationalen Sicherheit im Gegensatz zu anderen Interessen hätte, die nicht unter die Ausnahme fallen.

48. In dieser Hinsicht vertritt der EDSB die Auffassung, dass es der Mitteilung über die Wiederherstellung des Vertrauens gut getan hätte, bei der Festlegung der nächsten Schritte mehr Ehrgeiz an den Tag zu legen. Im Wortlaut werden keine präzisen Fristen genannt, mit Ausnahme der „Abhilfemaßnahmen", die bis zum Sommer 2014 erarbeitet und anschließend „möglichst umgehend" umgesetzt werden sollen[52]. Es wird nicht recht klar, was mit diesen Abhilfemaßnahmen gemeint ist. Sowohl im Bericht als auch in der Mitteilung werden Maßnahmen zur Verbesserung der Funktionsweise des Systems aufgeführt, und der EDSB empfiehlt der Kommission, genauer darzulegen, wie diese Maßnahmen in der Praxis umgesetzt werden könnten. Außerdem sollten der Inhalt und der Zeitplan des „allgemeinen Überprüfungsprozesses" besser festgelegt werden.

49. Bezüglich möglicher Verbesserungen des Safe-Harbour-Systems teilt der EDSB die Auffassung der Kommission, dass jede Reform auf die strukturellen Mängel bei der Transparenz und der Durchsetzung, die wichtigsten Grundsätze des Safe-Harbour-Systems und die Ausnahmeregelungen aus Gründen der nationalen Sicherheit ausgerichtet sein sollte.

50. Insbesondere begrüßt der EDSB die Aussagen, dass a) die US-Behörden gründlicher und systematischer überwachen und prüfen sollten, ob die Safe-Harbour Grundsätze beachtet werden, b) die Transparenz der Datenschutzgrundsätze, nach denen sich die beigetretenen Unternehmen richten, verbessert werden soll, c) EU-Bürger Zugang zu erschwinglichen Streitbeilegungsmechanismen haben sollten und d) die Ausnahmeregelung aus Gründen der nationalen Sicherheit nur in dringend notwendigen und angemessenen Fällen zur Anwendung kommen sollte.

51. Unabhängig von der gewählten strategischen Option sollten derzeit der Safe-Harbour-Regelung beigetretene Organisationen alle Grundsätze der Regelung einschließlich Transparenz beachten. Die US-Nachrichtendienste sollten allerdings auch nicht Ersuchen an Safe-Harbour-Mitglieder richten, die über das hinausgehen, was für Zwecke der nationalen Sicherheit unbedingt erforderlich ist und dazu in einem angemessenen Verhältnis steht.

52. Weiter hält der EDSB folgende Maßnahmen für erforderlich:
    a. Überarbeitung der „Häufig gestellten Fragen" (FAQ) zu den Safe-Harbour-Grundsätzen dahingehend, dass ihre Anwendung klargestellt und ihre praktischen Implikationen für Unternehmen, die der Regelung beitreten möchten, erläutert werden. Bei dieser Gelegenheit könnten auch die Modalitäten der Anwendung auf Auftragsverarbeiter insbesondere bei Weiterleitung der Daten klargestellt werden und könnte europäischen für die Verarbeitung Verantwortlichen eine größere Verantwortung bei der Kontrolle von in den USA angesiedelten Unternehmen daraufhin übertragen werden, ob sie die angeblich beachteten Safe-Harbour-Grundsätze auch tatsächlich einhalten;

[52] Siehe S. 7.

b. Einbeziehung europäischer Datenschutzbehörden in eine umfassende Kommunikationskampagne zum Thema „Safe Harbour“, nachdem die FAQs überarbeitet worden sind;
c. Aufforderung an die FTC, mehr Vor-Ort-Kontrollen durchzuführen und bei Verstößen gegen die Grundsätze schärfere Sanktionen zu verhängen;
d. nachdrückliches Hinweisen auf die Tatsache, dass die Safe-Harbour-Grundsätze nicht für den massenhaften Zugriff von US-Nachrichtendiensten auf Daten konzipiert wurden, die nach diesen Grundsätzen übermittelt werden.

III.3. Stärkung der Datenschutzgarantien im Bereich der strafrechtlichen Zusammenarbeit

53. Der Mitteilung über die Wiederherstellung des Vertrauens[53] ist zu entnehmen, dass gemäß dem Beschluss des Rates über die Ermächtigung der Kommission zur Aushandlung eines Rahmenabkommens über den Datenaustausch für Strafverfolgungszwecke zwischen der EU und den USA („Rahmenabkommen“), das nicht öffentlich zugänglich ist, die Verhandlungen darauf ausgerichtet sein sollen, „ein hohes Schutzniveau zu gewährleisten, das dem Besitzstand der EU im Bereich des Datenschutzes entspricht“.

54. Der EDSB begrüßt diese Zielsetzung, da ein solches Abkommen geeignet sein könnte, für den bestehenden oder künftigen Datenaustausch einen klareren Rahmen abzustecken und stärkere Datenschutzgarantien zu gewährleisten. Der EDSB hatte allerdings gewarnt, weil „durch einen solchen Rahmen eine massive Übermittlung von Daten in einem Bereich – nämlich bei der Strafverfolgung – sanktioniert werden könnte, in dem die Auswirkungen auf den Einzelnen besonders schwerwiegend sind und in dem verlässliche Schutzbestimmungen und Garantien umso mehr erforderlich sind“[54].

55. Auch an anderer Stelle hat der EDSB hierzu ausgeführt[55]: „Um Einheitlichkeit zu gewährleisten, sollte sich die EU zunächst über die Reform ihrer internen Datenschutzrechtsinstrumente einigen und auf der Grundlage dieses internen Regelwerks Abkommen mit Drittländern aushandeln“. Anschließend sollte dann ein Rahmenabkommen zwischen der EU und den USA über den Austausch personenbezogener Daten für Strafverfolgungszwecke die Grundlage für die Aushandlung sektorspezifischer Abkommen (z. B. PNR und TFTP) sein, nicht umgekehrt.

56. Mit Blick auf den aktuellen Kontext empfiehlt der EDSB, dafür zu sorgen, dass das künftige Datenschutzregelwerk auf sowohl auf allgemeiner als auch sektoraler Ebene bestehende Abkommen über den Austausch personenbezogener Daten für Strafverfolgungszwecke angewandt wird. Wie schon in seiner Stellungnahme zur Datenschutzreform empfiehlt der EDSB insbesondere, die Nicht-Anwendbarkeit des Datenschutzpakets zu befristen, die überdies nur für bestehende internationale

[53] Siehe S. 8.
[54] Siehe die Stellungnahme des EDSB vom 11. November 2008 zu dem Abschlussbericht der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten, abrufbar auf www.edps.europa.eu.
[55] Siehe z. B. die bereits zitierte Stellungnahme des EDSB zur Mitteilung der Kommission zum sektorübergreifenden Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer.

Abkommen gelten sollte. Außerdem sollten die vorgeschlagene Verordnung und die vorgeschlagene Richtlinie eine Übergangsklausel des Inhalts enthalten, dass die internationalen Abkommen innerhalb einer bestimmten Frist überprüft und an das Paket angepasst werden. Diese Klauseln sollten in den verfügenden Teil beider Vorschläge und nicht nur in deren Präambel aufgenommen werden[56].

57. Wie bereits ausgeführt, hinterfragt der EDSB auch die in der Mitteilung über die Wiederherstellung des Vertrauens wiederholte Aussage, dass das PNR- und das TFTP-Abkommen strenge Bedingungen für Datenübermittlungen und Garantien für EU-Bürger vorsehen.

58. In der Mitteilung über die Wiederherstellung des Vertrauens heißt es: „Die Verhandlungen bieten Gelegenheit festzulegen, dass auf personenbezogene Daten, die sich im Privatbesitz von Privatunternehmen in der EU befinden, von den US-Strafverfolgungsbehörden nicht außerhalb der offiziellen Kooperationskanäle zugegriffen wird bzw. dass diese Daten nicht außerhalb dieses Rahmens übertragen werden". Der EDSB begrüßt diese Versicherung. Weiter heißt es jedoch im Text: „Der Zugang über andere Wege ist nur in klar festgelegten und gerichtlich überprüfbaren Ausnahmefällen gestattet". Der EDSB empfiehlt, in der Mitteilung deutlich zum Ausdruck zu bringen, dass eine Ausnahme nur zugelassen wird, wenn sie unbedingt erforderlich und verhältnismäßig ist und im Einklang mit der ständigen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Gerichtshofs steht.

59. Bezüglich des Geltungsbereichs des Konzepts der nationalen Sicherheit, der auf der anderen Seite des Atlantiks möglicherweise anders gesehen wird, begrüßt der EDSB die Aussage, dass Ausnahmeregelungen aus Gründen der nationalen Sicherheit genau zu erläutern sind und dass hierzu gemeinsame Garantien und Beschränkungen festgelegt werden sollen.

60. Im Hinblick auf die in der Mitteilung erwähnten bzw. nicht erwähnten Garantien (wie Rechtsbehelfe) unterstützt der EDSB die Kommission in dem Ziel, feste Zusagen zu durchsetzbaren Rechten einschließlich gerichtlicher Rechtsbehelfsmechanismen für nicht in den USA ansässige EU-Bürger zu erhalten.

III.4. Berücksichtigung europäischer Belange im Rahmen des laufenden US-Reformprozesses

61. In der Mitteilung über die Wiederherstellung des Vertrauens[57] werden mögliche Verbesserungen am US-Rechtsrahmen erwähnt, mit denen vor allem Garantien für US-Bürger und in den USA ansässige EU-Bürger auf EU-Bürger ausgedehnt werden sollen, die nicht in den USA ansässig sind. Ferner sollen damit mehr Transparenz und bessere Aufsicht erreicht werden. Solche Änderungen sind natürlich zu begrüßen und zu unterstützen, weil sie vermutlich mehr und besseren Schutz für EU-Bürger und ihre Grundrechte, insbesondere im Hinblick auf Rechtsbehelfsmöglichkeiten, mit sich bringen.

[56] Siehe die Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, abrufbar auf www.edps.europa.eu.
[57] Siehe S. 9.

62. Gute Signale in diesem Zusammenhang sind der Bericht des *Privacy and Civil Liberties Oversight Board* vom 23. Januar 2014, die Rede von Präsident Obama vom 17. Januar 2014 und die Leitlinien des Präsidenten vom selben Tag. Weitere Änderungen wie die eben geforderten würden allerdings nicht nur das Vertrauen stärken und das Maß verringern, in dem Europäer von den Programmen betroffen sind, wie es in der Mitteilung heißt, sondern würden auch die Zahl der Fälle verringern, in denen Organisationen in einen Kompetenzkonflikt geraten können.

63. Gemäß der Mitteilung könnte mit solchen Änderungen „die Verarbeitung von für nationale Sicherheitsbelange unbedeutenden personenbezogenen Daten von Europäern eingeschränkt werden". Wie bereits ausgeführt, ist dieser Standard nach Ansicht des EDSB unangemessen; personenbezogene Daten von Europäern sollten aus Gründen der nationalen Sicherheit nur verarbeitet werden, wenn dies unbedingt erforderlich und verhältnismäßig ist.

64. Die EU sollte die US-Administration und den US-Kongress in ihren Bemühungen um ein allgemeines Datenschutzgesetz ermutigen und unterstützen, das starke Garantien und eine angemessene Aufsicht insbesondere in Bereichen vorsieht, in denen es derzeit an substanziellen Rechten auf Schutz der Privatsphäre mangelt.

65. Wie die Kommission begrüßt auch der EDSB die Stärkung des innerstaatlichen Rechtsrahmens der USA, insbesondere die im Februar 2012 von Präsident Obama angekündigte Annahme der „*Consumer Privacy Bill of Rights*" (Rechtekanon für den Verbraucherdatenschutz)[58]. Der EDSB fordert die EU-Organe auf, sich aktiv für die Verabschiedung eines umfassenden Datenschutzregelwerks in den USA einzusetzen, das den grenzüberschreitenden Datenverkehr erleichtern und gleichzeitig ein hohes Schutzniveau gewährleisten würde.

66. Als wichtige Interessenträger haben sich die US-Regierung und der private Sektor in den USA aktiv in die Diskussion über die Reform des EU-Datenschutzregelwerks eingebracht. Im Sinne von mehr Verständnis und Vertrauen und unter Berücksichtigung der Bedeutung der Übermittlungen zwischen der EU und den USA sollten sich auch die EU-Organe aktiv mit ihren Ansichten an der Debatte über das Datenschutzgesetz in den USA beteiligen.

III.5. TTIP-Verhandlungen

67. Die Kommission verweist auf die Verhandlungen zwischen der EU und den USA über eine transatlantische Handels- und Investitionspartnerschaft (*Transatlantic Trade and Investment Partnershi*p („TTIP")) und erklärt, dass Fragen der Datenschutzstandards nicht Gegenstand der Verhandlungen über die TTIP sind, „in deren Rahmen die Datenschutzbestimmungen uneingeschränkt eingehalten werden".

68. Der EDSB fordert die Kommission auf, zu gewährleisten, dass diese Zusage eingehalten wird und dass Fragen, die im Zusammenhang mit der TTIP erörtert

[58] Siehe „Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (Verbraucherdatenschutz in einer vernetzten Welt: ein Rahmen für den Schutz der Privatsphäre und zur Förderung von Innovation in der globalen digitalen Wirtschaft), White House, Februar 2012, abrufbar unter: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

werden könnten, wie „grenzüberschreitender Datenverkehr“[59], Standards und Zertifikate für die Cloud[60] oder Datensicherheitsanforderungen[61], sich nicht nachteilig auf den Schutz personenbezogener Daten auswirken. Gestützt insbesondere auf Artikel XIV des GATS sollte der Wortlaut des Abkommens eine Bestimmung enthalten, der zufolge es unbeschadet der anzuwendenden Datenschutzvorschriften gilt.

69. Gleichzeitig sollte die Kommission erwägen, ein gemeinsames Ziel der schrittweisen Entwicklung in Richtung einer größeren Interoperabilität der Regelwerke für Privatsphäre und Datenschutz festzulegen, ein Ziel, zu dessen Erreichen die USA in der unter Punkt 63 und 64 dargelegten Weise beitragen könnten.

III.6. Förderung von Datenschutznormen auf internationaler Ebene

70. Der EDSB unterstützt die Absicht der Kommission[62], auf internationaler Ebene EU-Vorschriften über die Erhebung, Verarbeitung und Übermittlung von Daten zu fördern. Der EDSB setzt sich insbesondere für die Annahme eines internationalen Instruments über die Einhaltung von Datenschutznormen bei nachrichtendienstlichen Tätigkeiten ein. Ein solches Instrument könnte auf UN-Ebene gestützt auf Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte angenommen werden[63].

71. Mit Blick auf die laufenden Diskussionen über das Übereinkommen des Europarates über Cyberkriminalität weist der EDSB nachdrücklich darauf hin, dass beim Zugriff von Strafverfolgungsbehörden von Drittländern auf Daten, die in den Zuständigkeitsbereich der EU fallen, die Datenschutzanforderungen der EU zu erfüllen sind[64].

72. Der EDSB schließt sich der Auffassung der Kommission an, dass die USA zur Förderung von Datenschutznormen auf internationaler Ebene am besten dem Übereinkommen des Europarates über den Schutz natürlicher Personen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) beitreten sollten, das auch Ländern offensteht, die nicht Mitglied des Europarates sind.

---

[59] Siehe die Kommentare der Kommission auf S. 4 des Berichts über den Dialog mit der Zivilgesellschaft – Das Neueste zu TTIP vom 16.7.2013, abrufbar unter http://trade.ec.europa.eu/doclib/docs/2013/july/tradoc_151656.pdf, zuletzt aufgerufen am 31.3.2014.

[60] Siehe die Kommentare der Kommission auf S. 2 des Berichts über das "TTIP Stakeholders Event“ vom 12.6.2013, http://ec.europa.eu/digital-agenda/en/news/ttip-ict-stakeholders-event-report, zuletzt aufgerufen am 31.3.2014.

[61] Siehe die Pressemitteilung der Kommission vom 20.12.2013 zur dritten Verhandlungsrunde, abrufbar unter http://trade.ec.europa.eu/doclib/press/index.cfm?id=1007, zuletzt aufgerufen am 31.3.2014.

[62] Siehe S. 9 der Mitteilung über die Wiederherstellung des Vertrauens.

[63] Siehe die Entschließung „Anchoring Data Protection and the Protection of Privacy in International Law“ (Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht), angenommen von der Internationalen Konferenz der Datenschutzbeauftragten (Warschau, 23.-26. September 2013).

[64] Siehe das Schreiben der Artikel 29-Datenschutzgruppe an den Ausschuss für Cyberkriminalität des Europarates vom 5. Dezember 2013, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf.

73. Nach Auffassung des EDSB sollten diese Bemühungen durch eine bessere Zusammenarbeit der Datenschutzbehörden und ihrer Durchsetzungsbehörden weltweit ergänzt werden[65]. Mit der Entwicklung internationaler Kooperationsmechanismen für die Durchsetzung sollte die Durchsetzung nationaler, regionaler und internationaler Datenschutzvorschriften im grenzüberschreitenden Kontext erleichtert werden.

III.7. Nachrichtendienstliche Tätigkeiten müssen angemessenen Garantien unterliegen

74. Nachrichtendienste und mit ihnen verbundene Stellen sind in einem lockerem Rahmen tätig, innerhalb dessen die Erfordernisse der Notwendigkeit und Verhältnismäßigkeit wichtiger denn je sind, jedoch nicht immer mit gesetzlich verankerten Garantien und Regelungen über eine angemessene Rechenschaftspflicht und Aufsicht berücksichtigt werden. Aufgrund der ständig zunehmenden Nutzung von Telekommunikationsnetzwerken durch Nutzer auf der ganzen Welt und des Einsatzes immer leistungsfähigerer technischer Mittel für die massive Erhebung und Speicherung von Daten können Nachrichtendienste immer mehr Daten abgreifen. Um diese gewachsene Macht zu bändigen, müssen auf allen Ebenen starke Garantien eingebaut werden und muss dafür gesorgt werden, dass die Überwachung notwendig ist und Eingriffe in das Recht auf Schutz des Privatlebens verhältnismäßig sind.

75. Nach Auffassung des EDSB wäre eine Garantie dafür, dass Überwachungstätigkeiten nicht über das erforderliche und verhältnismäßige Maß hinausgehen, eine stärkere Beaufsichtigung dieser nachrichtendienstlichen Tätigkeiten. Diese Beaufsichtigung sollte in unterschiedlicher Form auf unterschiedlichen Ebenen erfolgen:

- Im Augenblick der Durchführung einer Überwachungstätigkeit, die eine neue Verarbeitung bedeutet, würde das Erfordernis einer Genehmigung der Tätigkeit durch einen Richter oder eine andere unabhängige Behörde das Missbrauchsrisiko senken, weil dann gewährleistet wäre, dass Notwendigkeit und Verhältnismäßigkeit in dem Moment bestimmt werden, in dem Entscheidungen getroffen werden, die das Privatleben von Bürgern berühren. Die Genehmigung sollte eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Maßnahme enthalten, gegebenenfalls angemessene Garantien vorsehen und befristet sein.

- Die gesamte Verarbeitung sollte angemessen und wirksam von Parlamenten oder anderen zuständigen unabhängigen Einrichtungen beaufsichtigt werden. Das Mandat der Aufsichtsstellen sollte dahingehend erweitert werden, dass sie alle Aspekte der von allen Nachrichtendiensten vorgenommenen Verarbeitungen kontrollieren können.

- Auch der Datenaustausch zwischen Nachrichtendiensten verschiedener Länder sollte einer unabhängigen Aufsicht unterliegen.

[65] Siehe die Entschließung „International Enforcement Coordination“ (Internationale Koordinierung der Durchsetzung), angenommen von der Internationalen Konferenz der Datenschutzbeauftragten (Warschau, 23.-26. September 2013).

76. Den Aufsichtsstellen sollte die Aufgabe übertragen werden, die Anwendung der Datenschutzgrundsätze auf nachrichtendienstliche Tätigkeiten zu überwachen, und sie sollten hierfür angemessene Befugnisse erhalten. Bei der Kontrolle der Anwendung der Datenschutzgrundsätze sollte unter anderem auf Folgendes geachtet werden:

- Die Einrichtung strenger Kontrollen der Datenqualität: Fehlerrisiken treten auf, wenn private und öffentliche Datenbanken zusammengeführt werden (siehe PNR), und das so genannte „Data Mining" wirft ein Genauigkeitsproblem auf, das gelöst werden muss.

- Der Austausch personenbezogener Daten sollte regelmäßig im Hinblick auf die Bestimmung der Daten, den Zweck des Austauschs, die Qualität der Datenempfänger und die Frage überprüft werden, ob der Austausch in einem angemessenen Verhältnis zu seinem Eingriff in Grundrechte steht.

- Die Aufsichtsstellen sollten zusammenarbeiten. Hierzu ist es erforderlich, das bestehende Netz der Aufsichtsstellen dabei zu unterstützen, sich zu treffen und Informationen über gemeinsame Probleme und Lösungen für diese Probleme auszutauschen.

III.8. Gewährleistung wirksamer IT-Sicherheit

77. Die Gemeinschaft der Internetgestalter hat die Gefahren der massenhaften Überwachung erkannt und sich verpflichtet, abhörsicherere Infrastrukturen zu entwerfen und umzusetzen[66]. Europäische Forscher haben die Grundlagen für viele der wichtigsten Verschlüsselungsmechanismen geliefert. Softwareentwickler, insbesondere im Internet, sollten nicht nur der Verschlüsselung, sondern auch Risiken ihrer Produkte für die Privatsphäre besondere Aufmerksamkeit schenken und mit ihren Designmethoden konkret versuchen, diese Risiken zu vermeiden oder zumindest möglichst gering zu halten.

78. Die EU sollte ihre Stärken und Schwächen in diesem Bereich analysieren und ihre Initiativen in den Bereichen Forschung, Entwicklung und Bildung mit dem Ziel überprüfen, für jedermann wirksame und vertrauenswürdige Sicherheits-Tools bereitzustellen, und Entwickler darin schulen, Systeme zu entwerfen, die die Privatsphäre schützen. Der EDSB unterstützt den Austausch zu diesem Thema mit relevanten Akteuren[67].

IV. SCHLUSSBEMERKUNGEN

79. Der EDSB begrüßt die von der Kommission erwogenen Maßnahmen, weist jedoch darauf hin, dass die enthüllten Überwachungstätigkeiten von US-Nachrichtendiensten nicht nur das Vertrauen im Datenverkehr zwischen der EU und den USA beeinträchtigen. Sie wirken sich auch auf bestehende und durchsetzbare Rechte von EU-Bürgern auf Achtung ihrer Privatsphäre und den Schutz ihrer personenbezogenen Daten aus. Diese Rechte sind im Primär- und Sekundärrecht sowohl der EU als auch

[66] Vancouver IETF, https://www.ietf.org/media/2013-11-07-internet-privacy-and-security.html;
[67] https://www.w3.org/2014/strint/papers/64.pdf

des Europarates verankert. Der EDSB bedauert daher, dass in der Mitteilung über die Wiederherstellung des Vertrauens den Auswirkungen bestehender Rechtsinstrumente nicht mehr Raum gegeben wurde.

80. Der EDSB spricht sich dafür aus, dass sich die Kommission bei der Festlegung der nächsten Schritte in mehreren Punkten ehrgeiziger zeigt und merkt hierzu an:

- Eine korrekte Anwendung und Durchsetzung des derzeitigen europäischen Datenschutzregelwerks ist nicht nur gesetzlich vorgeschrieben, sondern wäre auch ein wesentlicher Beitrag zur Wiederherstellung des Vertrauens. Dies gilt auch für die Instrumente, in denen internationale Übermittlungen zwischen der EU und den USA geregelt sind, einschließlich der bestehenden Safe-Harbour-Grundsätze.

- Die Kommission sollte bedenken, dass Ausnahmen oder Einschränkungen von Grundrechten aus Gründen der nationalen Sicherheit nur gerechtfertigt und zulässig sind, wenn sie unbedingt erforderlich und verhältnismäßig sind und im Einklang mit der Rechtsprechung des EGMR und des Gerichtshofs stehen.

- Der EDSB stimmt voll und ganz der Aussage zu, dass für eine Konsolidierung und Verbesserung des EU-Datenschutzregelwerks eine zügige Annahme der Datenschutzreformvorschläge mit angemessenem Inhalt erforderlich ist, damit im Bereich des gesamten EU-Rechts ein stärkerer, wirksamerer und kohärenterer Schutz personenbezogener Daten und der Privatsphäre gegeben ist. Damit sollte auch ein angemessener Datenschutz bei einer Weiterverwendung der Daten für Strafverfolgungszwecke und bei internationalen Kompetenzkonflikten gewährleistet sein.

- Die Safe-Harbour-Grundsätze sollten in der von der Kommission angeregten Weise überarbeitet und gestärkt werden. Der EDSB empfiehlt die Vorgabe kürzerer Fristen, innerhalb derer diese Maßnahmen einschließlich angemessener Folgemaßnahmen bei verbleibenden Mängeln durchzuführen sind.

- Die Datenschutzgarantien für die Zusammenarbeit zwischen EU und USA im Bereich Strafverfolgung sind zu stärken. Die laufenden Verhandlungen über ein „Rahmenabkommen“ sollten keine massenhaften Datenübermittlungen legitimieren, sondern dem bestehenden Datenschutzrahmen und dem Ergebnis seiner derzeitigen Überprüfung Rechnung tragen. Es sollten insbesondere allen betroffenen Personen wirksame Rechtsbehelfsmechanismen zur Verfügung stehen, unabhängig von ihrer Staatsangehörigkeit. Dies sollte zu gegebener Zeit auch für internationale Abkommen gelten, bei Bedarf auf der Grundlage angemessener Übergangsklauseln.

- Die Kommission sollte die US-Administration und den US-Kongress in deren Bemühungen um ein allgemeines Datenschutzgesetz unterstützen, das starke Garantien und eine angemessene Aufsicht vorsieht, insbesondere in Bereichen, in denen es derzeit noch an einem substanziellen Schutz der Privatsphäre mangelt.

- Die derzeit stattfindenden Verhandlungen über eine TTIP sollten sich nicht nachteilig auf den Schutz personenbezogener Daten von Bürgern auswirken. Gleichzeitig sollte die Kommission erwägen, ein gemeinsames Ziel der schrittweisen Entwicklung in Richtung einer größeren Interoperabilität der Regelwerke für Privatsphäre und Datenschutz festzulegen, ein Ziel, zu dessen Erreichen die USA in der oben dargestellten Weise beitragen könnten.

- Die Förderung von Datenschutznormen auf internationaler Ebene sollte Folgendes umfassen:
  i. Förderung der vollständigen Übereinstimmung neuer internationaler Instrumente mit dem europäischen Datenschutzregelwerk;
  ii. Förderung des Beitritts von Drittländern und hier vor allem der USA zum Übereinkommen Nr. 108 des Europarates;
  iii. Unterstützung der Annahme eines internationalen Instruments über die Beachtung von Datenschutznormen im Rahmen nachrichtendienstlicher Tätigkeiten. Dieses Instrument könnte auf UN-Ebene auf der Grundlage von Artikel 17 IPBPR angenommen werden.

- Bei Überwachungstätigkeiten sollte jederzeit die Verpflichtung bestehen, die Rechtsstaatlichkeit zu wahren und die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit in einer demokratischen Gesellschaft einzuhalten. Die Regelwerke auf allen relevanten Ebenen sollten daher diesbezüglich klargestellt und bei Bedarf ergänzt werden. Diese Regelwerke sollten angemessene und hinreichend strenge Aufsichtsmechanismen umfassen.

- EU-Organe und alle einschlägigen Einrichtungen in den Mitgliedstaaten sind in ihrer Rolle als für die Verarbeitung Verantwortliche auch unmittelbar für die Gewährleistung einer wirksamen IT-Sicherheit verantwortlich. Dazu gehört, dass sie auf angemessener Ebene Datensicherheitsrisikobewertungen durchführen. Ferner sollten sie daher die Forschung zu Verschlüsselungsmechanismen fördern und bei für die Verarbeitung Verantwortlichen und Bürgern das Bewusstsein für die Risiken der verkauften oder verwendeten Produkte schärfen und von Entwicklern den Einsatz konkreter Designmethoden verlangen, mit denen sich diese Risiken vermeiden oder zumindest verringern lassen. Die EU sollte Aufklärungsinitiativen zur Sicherheit von im Internet verarbeiteten Daten durchführen.

Brüssel, den 20. Februar 2014

(**unterzeichnet**)

Peter HUSTINX
Europäischer Datenschutzbeauftragter