I

(Entschließungen, Empfehlungen und Stellungnahmen)

STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Abschlussbericht der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten

(2009/C 128/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

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

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

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 die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG — KONTEXT DER STELLUNGNAHME

1. Der Vorsitz des Rates der Europäischen Union hat dem Ausschuss der Ständigen Vertreter am 28. Mai 2008 im Hinblick auf das Gipfeltreffen am 12. Juni 2008 mitgeteilt, dass die hochrangige Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten ihren Bericht fertiggestellt hat. Dieser Bericht wurde am 26. Juni 2008 veröffentlicht [1].

2. Der Bericht zielt darauf ab, in einem ersten Schritt auf dem Weg zu einem Informationsaustausch mit den Vereinigten Staaten zur Bekämpfung von Terrorismus und schwerer grenzüberschreitender Kriminalität gemeinsame Grundsätze für den Schutz der Privatsphäre und den Datenschutz festzuhalten.

3. In der Mitteilung über das Vorliegen des Berichts erklärte der Ratsvorsitz, dass er Überlegungen zu der Frage begrüßen würde, welche Maßnahmen im Anschluss an diesen Bericht zu treffen wären; insbesondere bat er um Reaktionen auf die in dem Bericht ausgesprochenen Empfehlungen zum weiteren Vorgehen. Der Europäische Datenschutzbeauftragte (EDSB) ist dieser Aufforderung nachgekommen. Seine Stellungnahme basiert auf dem derzeitigen Stand der Beratungen, wie er aus dem veröffentlichten Bericht hervorgeht, und präjudiziert in keiner Weise Standpunkte, die er angesichts der weiteren Entwicklungen in Zukunft in dieser Frage möglicherweise vertreten wird.

4. Der EDSB stellt fest, dass die Beratungen der hochrangigen Kontaktgruppe in einem Kontext stattgefunden haben, in dem insbesondere seit dem 11. September 2001 der Datenaustausch zwischen den Vereinigten Staaten und der Europäischen Union durch internationale Abkommen und Übereinkünfte anderer Art weiterentwickelt wurde. Hierzu zählen die Abkommen von Europol und Eurojust mit den Vereinigten Staaten, die Abkommen zu den Fluggastdatensätzen (PNR-Abkommen) und der Fall SWIFT, der zu einem Briefwechsel zwischen EU- und US-Beamten führte, dessen Ziel die Festlegung von Mindestgarantien für den Datenschutz war [2].

[1] Ratsdokument Nr. 9831/08, englische Fassung abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

[2] — Agreement between the United States of America and the European Police Office of 6 December 2001, and Supplemental agreement between Europol and the USA on exchange of personal data and related information (Abkommen zwischen den Vereinigten Staaten von Amerika und dem Europäischen Polizeiamt vom 6. Dezember 2001 und Ergänzendes Abkommen zwischen Europol und den USA über den Austausch personenbezogener Daten und zugehöriger Informationen), in englischer Fassung abrufbar auf der Website von Europol;
— Agreement between the United States of America and Eurojust on judicial cooperation (Abkommen zwischen den Vereinigten Staaten von Amerika und Eurojust zur justiziellen Zusammenarbeit) vom 6. November 2006, englische Fassung abrufbar auf der Website von Eurojust;
— Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007), unterzeichnet in Brüssel am 23. Juli 2007 und in Wahington am 26. Juli 2007, ABl. L 204 vom 4.8.2007, S. 18.
— Briefwechsel zwischen den Behörden der Vereinigten Staaten und der EU über das Programm zum Aufspüren der Finanzierung des Terrorismus, 28. Juni 2007.

5. Darüber hinaus handelt die EU vergleichbare Übereinkünfte über den Austausch personenbezogener Daten mit anderen Drittländern aus und billigt diese. Ein jüngeres Beispiel hierfür ist das Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) aus der Europäischen Union und deren Übermittlung durch die Fluggesellschaften an die australische Zollbehörde ([3]).

6. In diesem Zusammenhang ist festzustellen, dass die Ersuchen der Strafverfolgungsbehörden von Drittländern um personenbezogene Informationen stetig zunehmen und nicht mehr nur Informationen betreffen, die in den üblichen Behörden-Datenbanken gespeichert sind, sondern auch andere Arten von Dateien, insbesondere solche, die von der Privatwirtschaft erhobene Daten enthalten.

7. Der EDSB weist als wichtige Hintergrundinformation darauf hin, dass die Frage der Übermittlung personenbezogener Daten an Drittländer im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in dem Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden ([4]), geregelt wird; dieser dürfte noch vor Ablauf des Jahres 2008 angenommen werden.

8. Es ist jedenfalls zu erwarten, dass der transatlantische Informationsaustausch ausgeweitet wird und dass weitere Bereiche, in denen personenbezogene Daten verarbeitet werden, in ihn einbezogen werden. In diesem Umfeld ist ein Dialog über „transatlantische Strafverfolgung" ebenso begrüßenswert wie heikel. Begrüßenswert, weil dadurch ein besser abgegrenzter Rahmen für den bereits erfolgenden oder künftigen Datenaustausch geschaffen werden könnte. Aber auch heikel, 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 ([5]).

9. Im folgenden Kapitel dieser Stellungnahme wird auf den gegenwärtigen Stand der Beratungen und das mögliche weitere Vorgehen eingegangen. Kapitel III hat den Anwendungsbereich und die Art der Übereinkunft, die eine gemeinsame Nutzung von Informationen ermöglichen soll, zum Gegenstand. In Kapitel IV werden Rechtsfragen, die mit dem Inhalt eines etwaigen Abkommens in Zusammenhang stehen, unter allgemeinen Gesichtspunkten analysiert. Zum einen wird darin der Frage nachgegangen, welche Bedingungen für die Bewertung des in den Vereinigten Staaten gewährleisteten Schutzniveaus gelten, zum anderen wird die Frage erörtert, ob der Rechtsrahmen der EU als Maßstab für die Bewertung dieses Schutzniveaus herangezogen werden kann. Ferner werden in diesem Kapitel auch die grundlegenden Anforderungen aufgeführt, die an ein Abkommen in diesem Bereich zu stellen wären. In Kapitel V der Stellungnahme werden schließlich die in der Anlage zu dem Bericht dargelegten Grundsätze zum Datenschutz analysiert.

II. GEGENWÄRTIGER STAND DER BERATUNGEN UND MÖGLICHES WEITERES VORGEHEN

10. Nach Auffassung des EDSB ist der gegenwärtige Stand der Beratungen so einzuschätzen, dass gewisse Fortschritte bei der Festlegung gemeinsamer Standards für die gemeinsame Nutzung von Informationen und den Schutz der Privatsphäre und der personenbezogenen Daten erzielt wurden.

11. Die Vorbereitungsarbeit für ein wie auch immer gestaltetes Abkommen zwischen der EU und den Vereinigten Staaten ist jedoch noch nicht abgeschlossen. Hier sind noch weitere Beratungen notwendig. In dem Bericht der hochrangigen Kontaktgruppe werden einige noch offene Punkte aufgeführt, von denen der wichtigste die Frage des „Grundsatzes des Rechtsbehelfs" ist. Uneinigkeit besteht nach wie vor über den erforderlichen Umfang des Rechtsbehelfs ([6]). In Kapitel 3 des Berichts werden fünf weitere noch offene Punkte aufgeführt. Diese Stellungnahme wird verdeutlichen, dass über diese Punkte hinaus noch zahlreiche weitere Fragen nicht geklärt sind, so beispielsweise der Anwendungsbereich und die Art der Übereinkunft über die gemeinsame Nutzung von Informationen.

12. Da in dem Bericht der Option eines verbindlichen Abkommens der Vorzug gegeben wird — eine Auffassung, die der EDSB teilt — ist umso mehr ein überlegtes Vorgehen erforderlich. Weitere sorgfältige und gründliche vorbereitende Arbeit ist unerlässlich, bevor ein Abkommen geschlossen werden kann.

13. Schließlich sei noch angemerkt, dass es nach Auffassung des EDSB am besten wäre, wenn ein solches Abkommen nach dem Lissabonner Vertrag geschlossen würde, was natürlich davon abhängt, wann dieser in Kraft treten wird. Nach dem Lissabonner Vertrag würde nämlich keine Rechtsunsicherheit in Bezug auf die Abgrenzung zwischen den Säulen der EU entstehen. Darüber hinaus wären die uneingeschränkte Einbeziehung des Europäischen Parlaments und eine gerichtliche Kontrolle durch den Gerichtshof gewährleistet.

14. Unter diesen Umständen sollte am besten zunächst ein Fahrplan im Hinblick auf den etwaigen späteren Abschluss eines Abkommens vereinbart werden. Dieser Fahrplan könnte folgende Aspekte umfassen:

   — Leitlinien und einen Zeitplan für die weiteren Beratungen der hochrangigen Kontaktgruppe (oder anderer Gruppen),

   — zu einem frühen Zeitpunkt Erörterung grundlegender Fragen, wie beispielsweise Anwendungsbereich und Art des Abkommens, und eventuelle Einigung in diesen Fragen,

   — auf der Grundlage der in den grundlegenden Fragen gefundenen Einigung weitere Ausgestaltung der Grundsätze für den Datenschutz,

   — in verschiedenen Phasen des Verfahrens Einbeziehung der interessierten Kreise;

   — auf europäischer Seite Berücksichtigung der institutionellen Erfordernisse.

([3]) ABl. L 213 vom 8.8.2008, S. 49.

([4]) Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, in der Fassung vom 24. Juni 2008 abrufbar unter http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Auf die Notwendigkeit eines eindeutigen Rechtsrahmens wird in den Kapiteln III und IV dieser Stellungnahme näher eingegangen.

([6]) S. Buchstabe C auf Seite 5 des Berichts.

III. **ANWENDUNGSBEREICH UND ART EINER ÜBEREINKUNFT ÜBER DIE GEMEINSAME NUTZUNG VON INFORMATIONEN**

15. Nach Auffassung des EDSB ist es von entscheidender Bedeutung, dass der Anwendungsbereich und die Art einer etwaigen Übereinkunft sowie die Grundsätze für den Datenschutz in einem ersten Schritt vor der weiteren Ausgestaltung einer solchen Übereinkunft eindeutig festgelegt werden.

16. Bezüglich des Anwendungsbereichs stellen sich folgende wichtige Fragen:

— Welche Akteure sind innerhalb und außerhalb des Strafverfolgungsbereichs beteiligt?

— Was ist unter dem „Zweck der Strafverfolgung" zu verstehen, und in welchem Verhältnis steht dieser Zweck zu anderen Zwecken wie nationale Sicherheit und insbesondere Grenzschutz und Gesundheitswesen?

— Wie fügt sich diese Übereinkunft in die Thematik eines umfassenden transatlantischen Raums der Sicherheit ein?

17. Bei der Festlegung der Art der Übereinkunft sollten folgende Fragen geklärt werden:

— Falls dies von Belang ist: im Rahmen welcher Säule werden die Verhandlungen über die Übereinkunft geführt?

— Wird es sich um eine für die EU und die Vereinigten Staaten verbindliche Übereinkunft handeln?

— Wird die Übereinkunft direkte Wirkung entfalten in dem Sinne, dass sie Rechte und Pflichten für Einzelpersonen festschreibt, die vor Gericht durchgesetzt werden können?

— Wird der Informationsaustausch in der Übereinkunft selbst geregelt, oder werden darin lediglich Mindeststandards für den Informationsaustausch festgelegt, die durch spezifische Vereinbarungen ergänzt werden müssen?

— In welcher Beziehung wird diese Übereinkunft zu geltenden Übereinkünften stehen? Wird sie diese einhalten, ersetzen oder ergänzen?

III. 1. **Anwendungsbereich der Übereinkunft**

Beteiligte Akteure

18. Der Bericht der hochrangigen Kontaktgruppe enthält zwar keine eindeutigen Festlegungen zu dem exakten Anwendungsbereich der künftigen Übereinkunft, die darin aufgeführten Grundsätze lassen jedoch den Schluss zu, dass sowohl die Datenübermittlung zwischen privatwirtschaftlichen und öffentlichen ([7]) Akteuren als auch die Datenübermittlung zwischen Behörden unter die Übereinkunft fallen sollen.

([7]) Siehe hierzu insbesondere Kapitel 3 des Berichts „Outstanding issues pertinent to transatlantic relations", Nummer 1 „Consistency in private entities' obligations during data transfers".

— Datenübermittlung zwischen privatwirtschaftlichen und öffentlichen Akteuren:

19. Der EDSB kann nachvollziehen, warum die künftige Übereinkunft auf die Datenübermittlung zwischen privatwirtschaftlichen und öffentlichen Akteuren anwendbar sein soll. Die Übereinkunft wird ausgearbeitet, weil in den letzten Jahren Ersuchen von US-Seite um Informationen von privatwirtschaftlichen Akteuren vorlagen. Der EDSB stellt in der Tat fest, dass privatwirtschaftliche Akteure sowohl auf EU-Ebene als auch auf internationaler Ebene vermehrt systematisch als Informationsquelle im Zusammenhang mit Strafverfolgungszwecken genutzt werden ([8]). Der Fall SWIFT war ein wichtiger Präzedenzfall, in dem ein privatwirtschaftliches Unternehmen aufgefordert war, systematisch große Mengen an Datensätzen an die Strafverfolgungsbehörden eines Drittlandes zu übermitteln ([9]). Das Abfragen von Fluggastdaten der Fluglinien folgt derselben Logik. Der EDSB hat die Rechtmäßigkeit dieser Entwicklung bereits in seiner Stellungnahme zu dem Entwurf eines Rahmenbeschlusses für ein europäisches System zur Verarbeitung von PNR-Daten in Frage gestellt ([10]).

20. Es sprechen noch zwei weitere Gründe dafür, der Aufnahme der Übermittlung von Daten zwischen privatwirtschaftlichen und öffentlichen Akteuren in den Anwendungsbereich eines künftigen Übereinkommens skeptisch gegenüberzustehen.

21. Zum einen könnte dies im Gebiet der EU selbst unerwünschte Wirkungen entfalten. Der EDSB befürchtet ernstlich, dass die Möglichkeit, Daten von privatwirtschaftlichen Unternehmen (z. B. von Finanzinstituten) an Drittländer zu übermitteln, starken Druck dahingehend erzeugen kann, dass dieselben Arten von Daten auch innerhalb der EU den Strafverfolgungsbehörden zur Verfügung zu stellen wären. Das PNR-System ist ein Beispiel für eine solche nicht wünschenswerte Entwicklung, die mit einer Sammelerhebung von Fluggastdaten durch die Vereinigten Staaten begann und dann auch auf den innereuropäischen Kontext übertragen wurde ([11]), ohne dass die Notwendigkeit und die Verhältnismäßigkeit eines solchen Systems eindeutig nachgewiesen worden wären.

22. Zum anderen hat der EDSB in seiner Stellungnahme zu dem Kommissionsvorschlag bezüglich eines PNR-Systems für die EU auch die Frage aufgeworfen, welcher

([8]) Siehe hierzu die Stellungnahme des EDSB vom 20. Dezember 2007 zu dem Entwurf eines Vorschlags für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, ABl. C 110 vom 1.5.2008, S. 1. „Traditionell besteht eine klare Trennung zwischen Strafverfolgungs- und privatwirtschaftlichen Tätigkeiten, wobei die Strafverfolgungsaufgaben von eigens dafür vorgesehenen Behörden — insbesondere Polizeibehörden — wahrgenommen werden, während privatwirtschaftliche Akteure auf Einzelfallbasis aufgefordert werden, diesen Strafverfolgungsbehörden personenbezogene Daten zu übermitteln. Die Tendenz geht nun dahin, dass private Akteure systematisch zur Mitarbeit zum Zwecke der Strafverfolgung verpflichtet werden,…"

([9]) Siehe Stellungnahme Nr. 10/2006 der Datenschutzgruppe vom 22. November 2006 zur Verarbeitung personenbezogener Daten bei der Society of Worldwide Interbank Financial Telecommunication (SWIFT), WP 128.

([10]) Stellungnahme vom 20. Dezember 2007, a.a.O.

([11]) Siehe hierzu den in Fußnote 8 genannten Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, der gegenwärtig im Rat erörtert wird.

Datenschutzrahmen (erste oder dritte Säule) auf die Bestimmungen anzuwenden wäre, denen eine Zusammenarbeit zwischen öffentlichen und privatwirtschaftlichen Akteuren unterliegen würde: Sollten die Vorschriften auf der Eigenschaft des für die Datenverarbeitung Verantwortlichen (Privatsektor) oder auf dem verfolgten Zweck (Strafverfolgung) beruhen? Zwischen der ersten und der dritten Säule gibt es in Fällen, in denen privatwirtschaftliche Akteure verpflichtet werden, personenbezogene Daten zu Strafverfolgungszwecken zu verarbeiten, keine eindeutige Abgrenzung. In diesem Zusammenhang ist es bezeichnend, dass Generalanwalt Bot in seinem Schlussantrag in einer Rechtssache zum Thema „Vorratsdatenspeicherung von Daten" ([12]) eine Grenzziehung für solche Fälle vorschlägt, aber gleich hinzufügt: „Diese Grenzziehung ist sicherlich nicht unumstritten und kann in mancher Hinsicht künstlich erscheinen." Der EDSB stellt zudem fest, dass auch in dem Beschluss des Gerichtshofs in der Rechtssache betreffend die Verarbeitung von Fluggastdatensätzen ([13]) die Frage nach dem geltenden Rechtsrahmen nicht vollständig beantwortet wird. Die Tatsache, dass bestimmte Aktivitäten nicht unter die Richtlinie 95/46/EG fallen, bedeutet beispielsweise nicht automatisch, dass diese Aktivitäten im Rahmen der dritten Säule geregelt werden können. Dies bedeutet, dass hier möglicherweise hinsichtlich des geltenden Rechts eine Lücke besteht, was in jedem Fall zu Rechtsunsicherheit hinsichtlich der für die Betroffenen bestehenden Rechtsgarantien führt.

23. Der EDSB hebt vor diesem Hintergrund hervor, dass sichergestellt sein muss, dass durch eine künftige — allgemeine Grundsätze für den Datenschutz enthaltende — Übereinkunft als solche die transatlantische Übermittlung personenbezogener Daten zwischen privatwirtschaftlichen und öffentlichen Akteuren nicht legitimiert werden darf. Eine solche Datenübermittlung kann nur dann in eine künftige Übereinkunft aufgenommen werden, wenn

   — in dieser künftigen Übereinkunft festgelegt wird, dass die Datenübermittlung nur dann zulässig ist, wenn sie für einen bestimmten Zweck nachweislich zwingend notwendig ist, wobei eine entsprechende Entscheidung von Fall zu Fall zu treffen wäre,

   — für die Übermittlung selbst hohe Datenschutzstandards (wie sie in dieser Stellungnahme beschrieben werden) gelten.

   Darüber hinaus weist der EDSB auf die bestehende Unsicherheit hinsichtlich des anwendbaren Datenschutzrahmens hin und spricht sich deshalb in jedem Fall dafür aus, die Übermittlung personenbezogener Daten zwischen privatwirtschaftlichen und öffentlichen Akteuren bei dem gegenwärtigen Stand der Rechtsvorschriften der EU nicht in die künftige Übereinkunft aufzunehmen.

   — Datenübermittlung zwischen Behörden:

24. Der Anwendungsbereich im Hinblick auf den Informationsaustausch ist nicht eindeutig abgegrenzt. In einem ersten Schritt in Richtung auf eine gemeinsame Übereinkunft sollte deren genauer Anwendungsbereich eindeutig festgelegt werden. Insbesondere folgende Fragen sind nach wie vor offen:

   — Soll die Übereinkunft bezüglich der in der EU bestehenden Datenbanken auf zentrale Datenbanken, die (teilweise) von der EU verwaltet werden — wie etwa die Datenbanken von Europol und Eurojust — anwendbar sein, oder auf dezentrale, von den Mitgliedstaaten verwaltete Datenbanken, oder auf beide Arten von Datenbanken?

   — Schließt der Anwendungsbereich der Übereinkunft zusammengeschaltete Netze ein, und gelten dann die vorgesehenen Sicherheitsgarantien für Daten, die zwischen den Mitgliedstaaten oder den Ämtern oder Agenturen ausgetauscht werden, in den Vereinigten Staaten ebenso wie in der EU?

   — Soll die Übereinkunft lediglich auf den Datenaustausch zwischen Datenbanken im Bereich der Strafverfolgung (Polizei, Justiz, eventuell Zoll) anwendbar sein, oder sollen auch andere Datenbanken, wie beispielsweise steuerliche Datenbanken, eingeschlossen sein?

   — Soll die Übereinkunft auch für die Datenbanken nationaler Sicherheitsbehörden gelten? Soll im Rahmen der Übereinkunft ein Zugriff dieser Behörden auf im Bereich der Strafverfolgung bestehende Datenbanken im Hoheitsgebiet der jeweils anderen Vertragspartei (Behörden der EU auf Datenbanken in den USA und umgekehrt), möglich sein?

   — Soll die Übereinkunft die Übermittlung von Informationen auf Einzelfallbasis abdecken, oder soll ein ständiger Zugriff auf bestehende Datenbanken vorgesehen werden? Diese letzte Annahme würde sicherlich Fragen nach der Verhältnismäßigkeit aufwerfen, auf die in Kapitel V unter Nummer 3 näher eingegangen wird.

Strafverfolgungszwecke

25. Die Definition des Zwecks eines etwaigen Abkommens lässt ebenfalls Raum für Unsicherheit. In der Einleitung und auch in dem ersten Grundsatz, der in der Anlage zum Bericht dargelegt ist, wird klar auf Strafverfolgungszwecke abgestellt; in Kapitel IV dieser Stellungnahme wird näher hierauf eingegangen. Der EDSB stellt fest, dass die genannten Textstellen darauf hindeuten, dass der Datenaustausch schwerpunktmäßig im Bereich der dritten Säule erfolgen soll; es stellt sich jedoch die Frage, ob es sich hierbei nicht lediglich um einen ersten Schritt in Richtung auf einen umfassenderen Informationsaustausch handelt. Es scheint eindeutig, dass die im Bericht genannten „Zwecke der öffentlichen Sicherheit" die Bekämpfung des Terrorismus, der organisierten Kriminalität und sonstiger Verbrechen einschließen. Soll das Abkommen aber darüber hinaus auch für den Datenaustausch in anderen Bereichen des öffentlichen Interesses gelten, wie etwa die Gefährdung der öffentlichen Gesundheit?

26. Der EDSB empfiehlt, den Zweck auf genau festgelegte Datenverarbeitungsvorgänge zu beschränken und die politischen Entscheidungen, die der Zweck-Definition zugrunde liegen, zu begründen.

([12]) Schlussantrag von Generalanwalt Bot vom 14. Oktober 2008 in der Rechtssache Irland gegen das Europäische Parlament und den Rat (Rechtssache C-301/06), Randnr. 108.

([13]) Urteil des Gerichtshofs vom 30. Mai 2006, Europäisches Parlament gegen Rat der Europäischen Union (C-317/04) und Kommission der Europäischen Gemeinschaften (C-318/04), verbundene Rechtssachen C-317/04 und C-318/04, Slg. I-2006 S. 4721.

Ein umfassender transatlantischer Raum der Sicherheit

27. Der gemäß dem Bericht vorgesehene breite Anwendungsbereich sollte vor dem Hintergrund des umfassenden transatlantischen Raums der Sicherheit, über den zur Zeit von der sogenannten Zukunftsgruppe ([14]) debattiert wird, betrachtet werden. Der im Juni 2008 veröffentlichte Bericht dieser Gruppe legt unter anderem einen Schwerpunkt auf die externe Dimension der Innenpolitik. Darin wird Folgendes empfohlen: „*Bis 2014 sollte die Europäische Union eine Entscheidung hinsichtlich des politischen Ziels treffen, im Bereich der Freiheit, der Sicherheit und des Rechts einen euro-atlantischen Raum der Zusammenarbeit mit den Vereinigten Staaten zu schaffen.*“ Eine solche Zusammenarbeit würde über Sicherheitsfragen im eigentlichen Sinne hinausgehen und mindestens die Themen umfassen, die in Titel IV EGV behandelt werden, wie Einwanderung, Visa- und Asylfragen und zivilrechtliche Zusammenarbeit. Hier muss die Frage gestellt werden, inwieweit eine Vereinbarung über grundlegende Datenschutz-Grundsätze, wie sie im Bericht der hochrangigen Kontaktgruppe aufgeführt sind, die Grundlage für einen Informationsaustausch in so einem so weit gefassten Bereich sein könnte oder sollte.

28. Normalerweise sollte im Jahr 2014 die Säulen-Struktur nicht mehr bestehen, und es dürfte eine einzige Rechtsgrundlage für den Datenschutz innerhalb der EU selbst geben (im Rahmen des Lissabonner Vertrags — Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union). Der Umstand, dass es eine Harmonisierung auf EU-Ebene hinsichtlich der *Regelung* des Datenschutzes gibt, bedeutet jedoch in keiner Weise, dass im Rahmen eines Abkommens mit einem Drittland die *Übermittlung* jedweder personenbezogener Daten, zu welchen Zwecken auch immer, zulässig wäre. Je nach Kontext und den Bedingungen, unter denen die Datenverarbeitung erfolgt, sind möglicherweise entsprechend angepasste Datenschutzgarantien für bestimmte Bereiche, wie beispielsweise den Bereich der Strafverfolgung, erforderlich. Der EDSB empfiehlt, bei der Ausarbeitung des künftigen Abkommens die Auswirkungen dieser verschiedenen Zusammenhänge zu berücksichtigen.

III.2. **Art des Abkommens**

Der europäische institutionelle Rahmen

29. Auf kurze Sicht ist es in jedem Fall unbedingt erforderlich, die Säule festzulegen, in deren Rahmen das Abkommen ausgehandelt werden soll. Dies ist insbesondere deswegen notwendig, weil sich ein solches Abkommen auf den internen Rechtsrahmen für den Datenschutz auswirken dürfte. Sollen die Verhandlungen im Rahmen der ersten Säule geführt werden, in der im wesentlichen die Richtlinie 95/46/EG gilt, die eine spezielle Regelung für die Übermittlung von Daten an Drittländer enthält, oder sollen die Verhandlungen im Rahmen der dritten Säule erfolgen, in der die Regeln für die Datenübermittlung an Drittländer weniger streng sind? ([15])

30. Zwar stehen, wie bereits erwähnt, Strafverfolgungszwecke im Vordergrund, in dem Bericht der hochrangigen Kontaktgruppe wird jedoch auch das Abfragen von Daten von privatwirtschaftlichen Akteuren genannt; ferner können die aufgeführten Zwecke auch in einem weiten Sinne dahingehend interpretiert werden, dass sie über reine Sicherheitsaspekte hinausgehen und beispielsweise Einwanderungs- und Grenzschutzfragen, aber auch das Gesundheitswesen einschließen können. Angesichts dieser Unwägbarkeiten wäre es von großem Vorteil, wenn die Harmonisierung der Säulen im EU-Recht, wie sie im Lissabonner Vertrag vorgesehen ist, abgewartet, die Rechtsgrundlage für die Verhandlungen eindeutig festgelegt und darüber hinaus genau festgelegt würde, welche Rolle den europäischen Organen, insbesondere dem Europäischen Parlament und der Kommission, zukommt.

Verbindlichkeit der Übereinkunft

31. Es sollte klargestellt werden, ob am Ende der Beratungen eine gemeinsame Vereinbarung oder eine andere nicht verbindliche Übereinkunft stehen soll, oder ob ein verbindliches internationales Abkommen geschlossen werden soll.

32. Der EDSB schließt sich dem Bericht an, in dem ein verbindliches Abkommen favorisiert wird. Nach Auffassung des EDSB ist ein offizielles verbindliches Abkommen eine unabdingbare Voraussetzung für eine Übermittlung von Daten aus der EU nach außen, unabhängig von dem Zweck, zu dem die Datenübermittlung erfolgt. Daten dürfen nur dann in ein Drittland übermittelt werden, wenn angemessene Regelungen getroffen und Schutzvorschriften festgelegt wurden, die Bestandteil eines speziellen (und verbindlichen) rechtlichen Rahmens sind. Mit anderen Worten: eine gemeinsame Absichtserklärung oder eine andere nicht verbindliche Übereinkunft können nützlich sein, um Leitlinien für die Verhandlungen im Hinblick auf ein weiteres verbindliches Abkommen zu bieten, vermögen jedoch niemals ein verbindliches Abkommen ersetzen.

Direkte Wirkung

33. Die Bestimmungen der Übereinkunft sollten gleichermaßen verbindlich für die Vereinigten Staaten und für die Europäische Union und ihre Mitgliedstaaten sein.

34. Darüber hinaus sollte sichergestellt werden, dass Einzelpersonen auf der Grundlage der vereinbarten Grundsätze ihre Rechte, und insbesondere das Recht auf Rechtsbehelf, wahrnehmen können. Der EDSB ist der Auffassung, dass dies am besten erreicht werden kann, wenn die materiellrechtlichen Bestimmungen der Übereinkunft so formuliert werden, dass sie unmittelbar für die Einwohner der Europäischen Union wirksam sind und vor Gericht geltend gemacht werden können. Deshalb müssen in der Übereinkunft die unmittelbare Wirksamkeit der Bestimmungen des internationalen Abkommens sowie die Bedingungen, die bei dessen Umsetzung in internes europäisches und nationales Recht erfüllt sein müssen, um die Wirksamkeit der Maßnahmen zu gewährleisten, eindeutig geregelt sein.

Verhältnis zu anderen Rechtsinstrumenten

35. Eine weitere grundlegende Frage ist, inwieweit das Abkommen eigenständig ist und inwieweit es auf Einzelfallbasis durch weitere Vereinbarungen zu spezifischen Datenaustauschfragen ergänzt werden muss. Es ist in der Tat fraglich, ob die mannigfaltigen Eigenheiten, die die Datenverarbeitung in der dritten Säule aufweist, durch ein

([14]) Bericht der Informellen Hochrangigen Beratenden Gruppe zur Zukunft der europäischen Innenpolitik „Freiheit, Sicherheit, Schutz der Privatsphäre — Europäische Innenpolitik in einer offenen Welt“ von Juni 2008, abrufbar im Verzeichnis der Ratsdokumente (register.consilium.europa.eu)

([15]) Siehe Artikel 11 und 13 des in Nummer 7 genannten Rahmenbeschlusses über den Schutz personenbezogener Daten.

einziges Abkommen in angemessener Weise mit einer einzigen Reihe von Normen abgedeckt werden können. Es ist noch fraglich, ob dieses einzige Abkommen ohne ergänzende Beratungen und Schutzbestimmungen die pauschale Billigung der Übermittlung personenbezogener Daten unabhängig vom Zweck der Übermittlung und der Art der übermittelten Daten überhaupt *zulassen* darf. Außerdem haben Abkommen mit Drittländern nicht unbedingt unbegrenzt Bestand, da sie an eine bestimmte Bedrohungslage gekoppelt sein, der Überprüfung unterliegen oder eine Auflösungsklausel beinhalten können. Andererseits könnten durch gemeinsame Mindeststandards, wie sie in einer verbindlichen Übereinkunft anerkannt würden, die weiteren Beratungen über die Übermittlung personenbezogener Daten im Zusammenhang mit einer spezifischen Datenbank oder mit spezifischen Datenverarbeitungsvorgängen erleichtert werden.

36. Der EDSB würde deshalb, wie es auch in dem Bericht der hochrangigen Kontaktgruppe dargelegt wurde, die Ausarbeitung von Mindestkriterien für den Datenschutz, die von Fall zu Fall durch ergänzende spezifische Bestimmungen vervollständigt werden, einem eigenständigen Abkommen vorziehen. Die ergänzenden spezifischen Bestimmungen sind die Voraussetzung für die Zulassung der Datenübermittlung in jedem Einzelfall. Hierdurch würde ein einheitliches Vorgehen beim Datenschutz gefördert.

Anwendung auf bestehenden Rechtsinstrumente

37. Es sollte überdies geprüft werden, wie ein etwaiges allgemeines Abkommen mit bereits bestehenden, zwischen der Europäischen Union und den Vereinigten Staaten geschlossenen Abkommen zusammenwirken würde. Hierbei sei darauf hingewiesen, dass diese bereits bestehenden Abkommen, unter denen besonders das PNR-Abkommen (dasjenige, das mehr Rechtssicherheit bietet), das Europol- und das Eurojust-Abkommen beziehungsweise der Briefwechsel in Sachen SWIFT hervorzuheben sind, nicht dasselbe Maß an Verbindlichkeit aufweisen ([16]). Würden diese bestehenden Übereinkünfte durch eine neue allgemeine Rahmenvereinbarung ergänzt, oder würden sie unverändert bestehen bleiben, da die neue Rahmenvereinbarung beim Austausch personenbezogener Daten lediglich auf künftige Vorgänge anzuwenden wäre? Nach Auffassung des EDSB wäre es aus Gründen der rechtlichen Kohärenz erforderlich, über harmonisierte Vorschriften zu verfügen, die sowohl auf geltende als auch auf künftige verbindliche Abkommen zur Datenübermittlung anwendbar wären und diese ergänzen würden.

38. Die Anwendung des allgemeinen Abkommens auf bestehende Übereinkünfte hätte den Vorteil, dass die Verbindlichkeit dieser Übereinkünfte gestärkt würde. Dies wäre insbesondere für solche Übereinkünfte wünschenswert, die nicht rechtlich verbindlich sind, wie beispielsweise der Briefwechsel im Fall SWIFT, da hierdurch wenigstens die Einhaltung einer Reihe allgemeiner Grundsätze für den Datenschutz vorgeschrieben würde.

IV. **ALLGEMEINE RECHTLICHE BEWERTUNG**

39. In diesem Kapitel wird der Frage nachgegangen, wie das durch eine bestimmte Rahmenvereinbarung oder Übereinkunft erreichte Schutzniveau zu bewerten ist; hierzu gehört auch die Frage nach den anzuwendenden Maßstäben und den notwendigen grundlegenden Anforderungen.

Angemessenes Schutzniveau

40. Nach Auffassung des EDSB dürfte klar sein, dass eines der wesentlichen Ergebnisse einer künftigen Übereinkunft darin bestehen sollte, dass die Übermittlung personenbezogener Daten an die Vereinigten Staaten nur dann erfolgen kann, wenn die US-Behörden ein angemessenes Schutzniveau gewährleisten (und umgekehrt).

41. Der EDSB ist der Meinung, dass hinreichende Garantien in Bezug auf das Schutzniveau für personenbezogene Daten lediglich durch eine Überprüfung der tatsächlichen Angemessenheit sichergestellt werden können. Seiner Auffassung nach wäre es für ein allgemeines Rahmenabkommen, dessen Anwendungsbereich so weit gefasst wäre wie in dem Bericht der hochrangigen Kontaktgruppe beschrieben, problematisch, einer solchen Überprüfung der tatsächlichen Angemessenheit standzuhalten. Die Angemessenheit des allgemeinen Abkommens kann nur dann anerkannt werden, wenn sie mit der Angemessenheit der spezifischen von Fall zu Fall getroffenen Vereinbarungen einhergeht.

42. Die Beurteilung des von Drittländern gewährleisteten Datenschutzniveaus ist keine ungewöhnliche Aufgabe, insbesondere nicht für die Europäische Kommission: in der ersten Säule ist die Angemessenheit des Schutzniveaus Voraussetzung für eine Datenübermittlung. Die Angemessenheit wurde verschiedentlich nach Artikel 25 der Richtlinie 95/46/EG unter Anwendung spezifischer Kriterien beurteilt und durch Entscheidungen der Europäischen Kommission bestätigt ([17]). In der dritten Säule sind derartige systematische Angemessenheitsüberprüfungen nicht ausdrücklich vorgesehen, eine Beurteilung der Angemessenheit des Schutzniveaus ist nur für die spezifischen Fälle nach Artikel 11 und 13 des noch nicht verabschiedeten Rahmenbeschlusses über den Schutz personenbezogener Daten ([18]) vorgeschrieben und bleibt den Mitgliedstaaten überlassen.

43. Im gegenwärtigen Fall betrifft der Anwendungsbereich Strafverfolgungszwecke; die Beratungen werden von der Kommission unter der Aufsicht des Rates geführt. Der Kontext ist ein anderer als bei der Beurteilung der *Safe Harbour* Grundsätze oder der Angemessenheit der kanadischen Rechtsvorschriften; er ist eher vergleichbar mit den jüngsten Verhandlungen über die Verarbeitung von Fluggastdaten mit den Vereinigten Staaten und Australien, die im rechtlichen Rahmen der dritten Säule geführt wurden. Die von der hochrangigen Kontaktgruppe aufgestellten Grundsätze wurden allerdings auch im Zusammenhang mit dem Programm für visumfreies Reisen genannt, das Grenzschutz- und Einwanderungsfragen und somit der ersten Säule zugeordnete Aspekte betrifft.

44. Der EDSB empfiehlt, dass bei der Beurteilung der Angemessenheit des durch die künftige Übereinkunft gewährleisteten Schutzniveaus die in diesen unterschiedlichen

([16]) Siehe Fußnote 2.

([17]) Entscheidungen der Kommission über die Angemessenheit des Schutzes personenbezogener Daten in Drittstaaten, einschließlich Argentinien, Kanada, der Schweiz, der Vereinigten Staaten, Guernsey, Isle of Man und Jersey sind abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm

([18]) Beschränkt auf Vorgänge, bei denen ein Mitgliedstaat an ein Drittland oder eine internationale Einrichtung Daten übermittelt, die ihm von den zuständigen Behörden eines anderen Mitgliedstaats übermittelt wurden.

Bereichen gewonnenen Erfahrungen berücksichtigt werden sollten. Er empfiehlt außerdem, den Begriff der „Angemessenheit" im Kontext einer künftigen Übereinkunft weiter zu entwickeln und hierbei Kriterien zugrunde zu legen, die den bei früheren Beurteilungen der Angemessenheit angewandten vergleichbar sind.

Gegenseitige Anerkennung — Gegenseitigkeit

45. Ein zweiter Aspekt des Schutzniveaus steht mit der gegenseitigen Anerkennung der Systeme der EU und der Vereinigten Staaten im Zusammenhang. In dem Bericht der hochrangigen Kontaktgruppe heißt es hierzu, dass das Ziel darin bestünde, in den Bereichen, für die diese Grundsätze gelten, die Anerkennung der Wirksamkeit der Regelungen beider Seiten für Datenschutz und Schutz der Privatsphäre zu erreichen ([19]) und eine gleichwertige und gegenseitige Anwendung der Rechtsvorschriften zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre zu erreichen.

46. Für den EDSB liegt es auf der Hand, dass die gegenseitige Anerkennung (oder Gegenseitigkeit) nur möglich ist, wenn ein angemessenes Schutzniveau gewährleistet wird. Mit anderen Worten, die künftige Übereinkunft sollte das Mindestschutzniveau harmonisieren (durch eine Beurteilung der Angemessenheit des Schutzniveaus, wobei zu berücksichtigen ist, dass auf Einzelfallbasis spezifische Vereinbarungen zu treffen sein werden). Nur unter dieser Voraussetzung kann die Gegenseitigkeit anerkannt werden.

47. Der erste dabei zu berücksichtigende Aspekt betrifft die Gegenseitigkeit materiellrechtlicher Bestimmung zum Datenschutz. Nach Ansicht des EDSB sollte bei einem Abkommen mit dem Konzept der Gegenseitigkeit materiellrechtlicher Bestimmungen zum Datenschutz in einer Weise umgegangen werden, die es erlaubt, einerseits dafür zu sorgen, dass die Datenverarbeitung innerhalb des Gebiets der EU (und der Vereinigten Staaten) unter uneingeschränkter Achtung der innerstaatlichen Rechtsvorschriften zum Datenschutz erfolgt, und andererseits sicherzustellen, dass eine Verarbeitung von Daten, die außerhalb des Herkunftsstaates der Daten erfolgt und in den Anwendungsbereich des Abkommens fällt, unter Achtung der im Abkommen enthaltenen Datenschutzgrundsätze durchgeführt wird.

48. Der zweite Aspekt ist die Gegenseitigkeit der Rechtsbehelfsmechanismen. Es muss sichergestellt sein, dass für europäische Bürger angemessene Rechtsbehelfe bestehen, wenn ihre Person betreffende Daten in den Vereinigten Staaten verarbeitet werden (unabhängig von den Rechtsvorschriften, die für diese Verarbeitung gelten), und dass umgekehrt die Europäische Union und ihre Mitgliedstaaten US-Bürgern die gleichen Möglichkeiten einräumen.

49. Ein dritter Aspekt ist die Gegenseitigkeit des Zugriffs auf personenbezogene Daten, der Strafverfolgungsbehörden gewährt wird. Sollte den Behörden der Vereinigten Staaten durch eine Übereinkunft Zugriff auf Daten gewährt werden, die aus der Europäischen Union stammen, würde Gegenseitigkeit bedeuten, dass den Behörden der Europäischen Union in derselben Weise Zugriff auf Daten gewährt wird, die aus den Vereinigten Staaten stammen. Diese Gegenseitigkeit darf die Wirksamkeit des Schutzes der Betroffenen nicht beeinträchtigen. Dies ist eine Voraussetzung dafür, dass ein „transatlantischer" Zugriff auf Daten durch Strafverfolgungsbehörden gestattet wird. Konkret bedeutet dies, dass

— ein unmittelbarer Zugriff durch Behörden der Vereinigten Staaten auf Daten, die im Hoheitsgebiet der EU verarbeitet werden (und umgekehrt), nicht gestattet werden sollte, und dass der Zugriff nur indirekt unter Verwendung eines Push-Systems gewährt werden sollte,

— der Zugriff unter der Aufsicht der Datenschutz- und der Justizbehörden des Landes, in dem die Daten verarbeitet werden, erfolgen sollte,

— beim Zugriff amerikanischer Behörden auf Datenbanken, die innerhalb der EU bestehen, die materiellrechtlichen Bestimmungen zum Datenschutz (siehe oben) eingehalten werden und für die Betroffenen uneingeschränkte Rechtsbehelfe bestehen sollten.

Ausführlichkeit der Übereinkunft

50. Die genaue Festlegung der Bewertungsbedingungen (Angemessenheit, Gleichwertigkeit, gegenseitige Anerkennung) ist von wesentlicher Bedeutung, da hierdurch der Inhalt im Hinblick auf Genauigkeit, Rechtssicherheit und Wirksamkeit des Schutzes bestimmt wird. Eine künftige Übereinkunft muss inhaltlich präzise und sorgfältig abgefasst sein.

51. Darüber hinaus sollte eindeutig festgelegt sein, dass in jede weitere spezifische Vereinbarung, die im weiteren getroffen wird, ausführliche und umfassende Datenschutzbestimmungen für den Bereich aufgenommen werden müssen, für den im Rahmen der Vereinbarung ein Datenaustausch vorgesehen ist. Nur durch eine Festlegung von konkreten Datenschutzgrundsätzen auf beiden Ebenen kann das erforderliche enge Ineinandergreifen von allgemeinem Abkommen und spezifischen Vereinbarungen, wie bereits in den Nummern 35 und 36 dieser Stellungnahme bemerkt wurde, sichergestellt werden.

Entwicklung eines Modells, das auf andere Drittländer anwendbar ist

52. Mit besonderer Aufmerksamkeit sollte geprüft werden, inwieweit ein Abkommen mit den Vereinigten Staaten als Modell für Abkommen mit anderen Drittländern dienen kann. Der EDSB weist darauf hin, dass in dem vorgenannten Bericht der Zukunftsgruppe neben den Vereinigten Staaten auch Russland als strategischer Partner der EU genannt wird. Soweit die Grundsätze neutral sind und mit den grundlegenden Schutzbestimmungen der EU übereinstimmen, können sie durchaus als nützliches Modell dienen. Besonderheiten jedoch, die beispielsweise mit dem Rechtsrahmen des empfangenden Landes oder dem Zweck der Datenübermittlung in Zusammenhang stehen, würden einer einfachen Übertragung des Abkommens entgegenstehen. Von ebenso entscheidender Bedeutung ist die Lage der Demokratie in Drittländern: es muss dafür gesorgt sein, dass die vereinbarten Grundsätze in dem empfangenden Land wirksam sichergestellt und umgesetzt werden.

Welche Maßstäbe sind zur Beurteilung des Schutzniveaus heranzuziehen?

53. Für eine implizite oder explizite Angemessenheit sollte generell eine Übereinstimmung mit dem internationalen und dem europäischen Rechtsrahmen und insbesondere eine Übereinstimmung mit den gemeinsam vereinbarten Datenschutzgarantien gegeben sein. Diese sind in den

([19]) Kapitel A. Binding international agreement (Verbindliches internationales Abkommen), S. 8.

Richtlinien der Vereinten Nationen, dem Übereinkommen 108 des Europarates und dem zugehörigen Zusatzprotokoll, den Richtlinien der OECD, dem Entwurf eines Rahmenbeschlusses über den Schutz personenbezogener Daten und — für den Bereich der ersten Säule — in der Richtlinie 95/46/EG ([20]) enthalten. Alle diese Übereinkünfte enthalten vergleichbare Grundsätze, die allgemein als Kerngrundsätze für den Schutz personenbezogener Daten anerkannt werden.

54. Angesichts der Auswirkungen, die eine potenzielle Übereinkunft in der von der hochrangigen Kontaktgruppe vorgesehenen Form haben kann, ist es umso wichtiger, dass die vorgenannten Grundsätze angemessen berücksichtigt werden. Eine Übereinkunft, die den gesamten *Strafverfolgungs*bereich eines Drittlandes berührt, wäre in der Tat ein bisher noch nicht aufgetretenes Ereignis. Bestehende Beschlüsse zur Angemessenheit im Rahmen der ersten Säule und Übereinkommen, die im Rahmen der dritten Säule der EU mit Drittländern geschlossen wurden (Europol, Eurojust) standen immer mit spezifischen Datenübermittlungsvorgängen im Zusammenhang; im vorliegenden Fall jedoch könnte der Anwendungsbereich für die Übermittlung von Daten möglicherweise sehr viel weiter gefasst werden, wenn man bedenkt, dass die Zielsetzung sehr breit angelegt ist (Bekämpfung von strafbaren Handlungen, nationale und öffentliche Sicherheit, Grenzschutz) und dass keine Klarheit über die Zahl der Datenbanken, die betroffen wären, besteht.

Grundlegende Anforderungen

55. Die Bedingungen, die im Zusammenhang mit der Übermittlung personenbezogener Daten an Drittländer eingehalten werden müssen, sind in einem Arbeitspapier der Datenschutzgruppe ([21]) ausgearbeitet worden. Jedwede Vereinbarung von Mindestgrundsätzen für den Datenschutz sollte einer Übereinstimmungsprüfung unterzogen werden, durch die die Wirksamkeit der Datenschutzgarantien sichergestellt wird.

— Zum Inhalt: Durch die Datenschutzgrundsätze sollte ein hohes Maß an Schutz sichergestellt werden; ferner sollten die Grundsätze mit den Normen übereinstimmen, die im Einklang mit den Grundsätzen der EU stehen. In dieser Stellungnahme werden die zwölf in dem Bericht der hochrangigen Kontaktgruppe genannten Grundsätze unter diesem Aspekt näher untersucht.

— Zur Spezifität: Entsprechend der Art des Abkommens — und insbesondere im Falle eines förmlichen internationalen Abkommens — müssen die Regeln und Verfahren hinreichend ausführlich festgelegt werden, um eine wirksame Umsetzung zu ermöglichen.

— Zur Aufsicht: Um sicherzustellen, dass die vereinbarten Regeln eingehalten werden, müssen spezifische Kontrollmechanismen vorgesehen werden, die sowohl interne Kontrollen (Audits) als auch externe Kontrollen (Überprüfungen) umfassen. Diese Mechanismen müssen beiden Vertragsparteien gleichermaßen zur Verfügung stehen. Die Aufsicht umfasst Mechanismen, durch die einerseits die Einhaltung auf Makroebene sichergestellt werden kann, wie beispielsweise Mechanismen zur gemeinsamen Überprüfung, und durch die andererseits auch für die Einhaltung auf der Mikroebene gesorgt werden kann, wie beispielsweise die Möglichkeit des Rechtsbehelfs für den Einzelnen.

56. Neben diesen drei grundlegenden Anforderungen muss auch den Besonderheiten, die sich aus der Verarbeitung personenbezogener Daten im Kontext der Strafverfolgung ergeben, spezielle Aufmerksamkeit gewidmet werden. Es handelt sich hierbei um einen Bereich, in dem fundamentale Rechte in gewissem Umfang eingeschränkt werden können. Deshalb müssen Schutzbestimmungen erlassen werden, durch die die Einschränkungen der Rechte des Einzelnen insbesondere bezüglich der nachstehenden Aspekte im Hinblick auf die Auswirkungen für den Einzelnen ausgeglichen werden:

— Transparenz: Die Informationen über die Erhebung personenbezogener Daten und der Zugang zu diesen Daten können im Kontext der Strafverfolgung aufgrund der Notwendigkeit nicht-öffentlicher Ermittlungen eingeschränkt werden. Während in der EU immer schon zusätzliche Mechanismen geschaffen wurden, um diese Einschränkung fundamentaler Rechte auszugleichen (oftmals durch Einbeziehung unabhängiger Datenschutzstellen), muss dafür gesorgt werden, dass entsprechende Ausgleichsmechanismen auch zur Verfügung stehen, wenn die entsprechenden Informationen an ein Drittland übermittelt werden.

— Rechtsbehelf: aus den vorgenannten Gründen sollten für Einzelpersonen verschiedene Möglichkeiten bestehen, ihre Rechte zu wahren, insbesondere durch Anrufung einer unabhängigen Aufsichtsbehörde oder eines Gerichts.

— Vorratsspeicherung von Daten: die Begründung für den Zeitraum der Vorratsspeicherung von Daten kann in Bezug auf ihre Transparenz zu wünschen übriglassen. Es sind Maßnahmen zu treffen, durch die sichergestellt wird, dass hierdurch die betroffenen Personen oder die Aufsichtsbehörden nicht in der effektiven Wahrnehmung ihrer Rechte eingeschränkt werden.

([20]) — Richtlinien zur Regelung von automatisierten personenbezogenen Dateien, verabschiedet von der Generalversammlung der VN am 14. Dezember 1990, engl. Fassung abrufbar unter www.unhchr.ch/html/menu3/b/71.htm
— Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates vom 28. Januar 1981, abrufbar unter http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm
— OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Richtlinien der OECD über den Schutz der Privatsphäre und den grenzüberschreitenden Datenverkehr) vom 23. September 1980, engl. Fassung abrufbar unter www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Entwurf eines Rahmenbeschlusses des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, in der Fassung abrufbar unter http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

([21]) Arbeitspapier vom 24. Juli 1998 über die Übermittlung personenbezogener Daten an Drittstaaten, Anwendung der Artikel 25 und 26 der Datenschutzrichtlinie der EU; WP12.

— Rechenschaftspflicht der Strafverfolgungsbehörden: Bei fehlender tatsächlicher Transparenz können die Kontrollmechanismen, die Einzelpersonen oder institutionellen Akteuren zur Verfügung stehen, keinesfalls umfassend sein. Angesichts der Sensibilität der Daten und angesichts der Zwangsmaßnahmen, die auf der Grundlage der Verarbeitung von Daten gegen Einzelpersonen ergriffen werden können, wäre es dennoch sehr wichtig, dass Kontrollen fest verankert sind. Die Rechenschaftspflicht ist von entscheidender Bedeutung, und dies nicht nur in Bezug auf nationale Kontrollmechanismen im Empfängerland, sondern auch in Bezug auf die Überprüfungsmöglichkeiten, die für das Herkunftsland oder die Herkunftsregion der Daten bestehen. Überprüfungsmechanismen sind in speziellen Abkommen, wie beispielsweise dem PNR-Abkommen, vorgesehen, und der EDSB empfiehlt nachdrücklich, sie auch in die allgemeine Übereinkunft aufzunehmen.

V. **ANALYSE DER GRUNDSÄTZE**

Einleitung

57. In diesem Kapitel werden die zwölf in dem Dokument der hochrangigen Kontaktgruppe enthaltenen Grundsätze unter folgenden Aspekten analysiert:

— Die Grundsätze machen deutlich, dass die Vereinigten Staaten und die EU in einigen Punkten bezüglich der Grundsätze gleiche Ansichten vertreten, da Ähnlichkeiten mit den Grundsätzen des Übereinkommens 108 festzustellen sind.

— Eine Einigung über die Grundsätze ist jedoch nicht ausreichend. Ein Rechtsinstrument sollte in einer Weise abgefasst sein, die seine Einhaltung sicherstellt.

— Der EDSB bedauert, dass den Grundsätzen keine Erläuterungen beigegeben wurden.

— Bevor die Grundsätze analysiert werden können, muss klargestellt sein, dass beide Seiten den verwendeten Wortlaut in gleicher Weise verstehen, insbesondere im Hinblick auf die Begriffe der personenbezogenen Information oder der geschützten Personen. Vorzugsweise sollten Begriffsbestimmungen hierzu aufgenommen werden.

1. Zweckbindung

58. Gemäß dem ersten in der Anlage zu dem Bericht der hochrangigen Kontaktgruppe aufgeführten Grundsatz hat die Verarbeitung personenbezogener Informationen zum Zwecke der rechtmäßigen Strafverfolgung zu erfolgen. Wie bereits erwähnt, versteht die Europäische Union darunter die Prävention, Feststellung, Ermittlung oder Verfolgung von strafbaren Handlungen. Gemäß dem Verständnis der Vereinigten Staaten geht der Begriff der Strafverfolgung über strafbare Handlungen hinaus und umfasst auch Zwecke des Grenzschutzes sowie der öffentlichen und der nationalen Sicherheit. Es ist unklar, welche Folgen diese Unstimmigkeit, die zwischen der EU und den Vereinigten Staaten in Bezug auf den verfolgten Zweck besteht, haben kann. Zwar heißt es in dem Bericht, dass die verfolgten Zwecke in der Praxis möglicherweise weitgehend deckungsgleich sind, dennoch ist es von entscheidender Bedeutung, dass Klarheit darüber besteht, in welchem Umfang sie sich *nicht* decken. Angesichts der Auswirkungen, die getroffene Maßnahmen auf Einzelpersonen haben können, muss im Bereich der Strafverfolgung der Grundsatz der Zweckbindung streng eingehalten werden. Der festgelegte Zweck muss eindeutig und eingegrenzt sein. In Anbetracht der im Bericht vorgesehenen Gegenseitigkeit scheint auch die Angleichung des von beiden Seiten verfolgten Zwecks von grundlegender Bedeutung. Kurz gesagt, es muss eindeutig präzisiert werden, wie dieser Grundsatz zu verstehen ist.

2. Vollständigkeit/Datenqualität

59. Der EDSB begrüßt die Bestimmung, wonach für eine gesetzmäßige Verarbeitung personenbezogener Informationen deren sachliche Richtigkeit, Relevanz, Aktualität und Vollständigkeit Voraussetzung ist. Dieser Grundsatz ist eine Grundvoraussetzung für eine effiziente Verarbeitung von Daten.

3. Notwendigkeit/Verhältnismäßigkeit

60. Dieser Grundsatz stellt einen eindeutigen Zusammenhang zwischen der erhobenen Information und der Notwendigkeit dieser Information für gesetzlich festgelegte Strafverfolgungszwecke her. Diese Forderung nach einer Rechtsgrundlage ist eine positive Komponente der Gewährleistung der Rechtmäßigkeit der Verarbeitung der Daten. Der EDSB weist dennoch darauf hin, dass hierdurch zwar für mehr Rechtssicherheit bei der Verarbeitung gesorgt wird, die Rechtsgrundlage für die Verarbeitung jedoch in einem Gesetz eines Drittlandes besteht. Ein Gesetz eines Drittlandes an sich kann nicht die rechtmäßige Grundlage für die Übermittlung personenbezogener Daten darstellen ([22]). Im Kontext des Berichts der hochrangigen Kontaktgruppe wird anscheinend die Rechtmäßigkeit des Gesetzes eines Drittlandes, d.h. der Vereinigten Staaten, grundsätzlich anerkannt. In diesem Zusammenhang muss berücksichtigt werden, dass diese Argumentation — selbst wenn sie in diesem Fall gerechtfertigt sein mag, da es sich bei den Vereinigten Staaten um einen demokratischen Staat handelt — in keiner Weise für die Beziehungen mit anderen Drittländern gelten und auch nicht auf diese Beziehungen übertragen werden kann.

61. Die Übermittlung personenbezogener Daten muss gemäß der Anlage zu dem Bericht der hochrangigen Kontaktgruppe relevant, notwendig und angemessen sein. Der EDSB hebt hervor, dass im Rahmen der Verarbeitung nicht unangemessen stark in die Privatsphäre eingedrungen werden darf und dass die Verarbeitungsmodalitäten ausgewogen sein und den Rechten und Interessen der betroffenen Person Rechnung tragen müssen.

62. Deshalb sollte der Zugang zu Informationen für jeden Einzelfall geregelt werden, je nach dem konkreten Bedarf im Rahmen einer spezifischen Ermittlung. Ein ständiger Zugriff auf Datenbanken in der EU durch die Strafverfolgungsbehörden eines Drittlandes wäre als unangemessen und nicht hinlänglich gerechtfertigt zu betrachten. Der EDSB weist darauf hin, dass selbst im Kontext bestehender Abkommen zum Datenaustausch, wie beispielsweise im Fall des PNR-Abkommens, der Austausch von Daten auf der Grundlage

([22]) Siehe insbesondere Artikel 7 Buchstaben c und e der Richtlinie 95/46/EG. Die Datenschutzgruppe hat in ihrer Stellungnahme 6/2002 vom 24. Oktober 2002 zur Übermittlung von Angaben aus dem Fluggastverzeichnis durch Fluglinien an die Vereinigten Staaten festgehalten, dass es nicht tragbar erscheint, dass eine von einem Drittstaat aus Gründen des eigenen öffentlichen Interesses getroffene einseitige Entscheidung dazu führt, dass eine routinemäßige und pauschale Übermittlung von Daten erfolgt, die gemäß der Richtlinie geschützt sind.

bestimmter Umstände erfolgt, und dass dieses Abkommen für einen begrenzten Zeitraum abgeschlossen wurde ([23]).

63. Im gleichen Sinne sollte die Zeitdauer der Vorratsspeicherung von Daten geregelt sein: Daten sollten nur so lange gespeichert werden, wie sie in Anbetracht des verfolgten spezifischen Zwecks benötigt werden. Sind sie für den festgelegten Zweck nicht mehr relevant, sollten sie gelöscht werden. Der EDSB ist strikt gegen den Aufbau von Datenspeichern, in denen Angaben zu unverdächtigen Einzelpersonen in der Überlegung gespeichert werden, dass diese Angaben möglicherweise zu einem späteren Zeitpunkt noch einmal gebraucht werden könnten.

4. Informationssicherheit

64. Gemäß den Grundsätzen sind Maßnahmen und Verfahren vorgesehen, durch die Daten vor Missbrauch, Abänderung und sonstigen Gefahren geschützt werden sollen; ferner ist eine Bestimmung vorgesehen, durch die der Zugriff auf die Daten befugten Personen vorbehalten wird. Der EDSB hält dies für zufriedenstellend.

65. Der Grundsatz könnte darüber hinaus um eine Bestimmung ergänzt werden, wonach Aufzeichnungen darüber zu führen wären, wer auf die Daten zugegriffen hat. Hierdurch würde den Schutzbestimmungen zur Beschränkung des Zugriffs auf Daten und zur Verhinderung des Datenmissbrauchs mehr Wirksamkeit verliehen.

66. Überdies sollte vorgesehen werden, dass sich die Parteien im Fall von Sicherheitsverletzungen gegenseitig informieren: die Datenempfänger in den Vereinigten Staaten und in der EU wären dafür zuständig, die jeweils andere Seite davon in Kenntnis zu setzen, wenn die Daten, die ihnen übermittelt wurden, unrechtmäßig offengelegt wurden. Hierdurch wird zu mehr Verantwortung für eine sichere Verarbeitung der Daten beigetragen.

5. Besondere Kategorien personenbezogener Informationen

67. Nach Auffassung des EDSB wird der Grundsatz, der die Verarbeitung sensibler Daten verbietet, durch die Ausnahmeregelung, nach der eine Verarbeitung sensibler Daten zulässig ist, sofern die nationalen Rechtsvorschriften „geeignete Schutzbestimmungen" vorsehen, erheblich abgeschwächt. Gerade weil es sich um sensible Informationen handelt, muss jede Ausnahmeregelung vom Verbotsgrundsatz angemessen sein und genau begründet werden; diese Begründung muss nicht nur eine Auflistung der Zwecke, zu denen bestimmte Arten von sensiblen Daten verarbeitet werden können, und der Umstände, unter denen eine solche Verarbeitung erfolgen kann, umfassen, sondern auch Angaben zur Eigenschaft der betreffenden zur Verarbeitung dieser Daten ermächtigten Verantwortlichen enthalten. Nach Auffassung des EDSB sollte es Bestandteil der zu vereinbarenden Schutzbestimmungen sein, dass sensible Daten an sich kein Faktor sein dürfen, der Ermittlungen auslöst. Sensible Daten könnten unter bestimmten Umständen zur Verfügung gestellt werden, jedoch lediglich als ergänzende Informationen zu einer betroffenen Person, gegen die bereits Ermittlungen eingeleitet wurden. Der Wortlaut des Grundsatzes muss eine erschöpfende Aufzählung dieser Schutzbestimmungen und Bedingungen enthalten.

6. Rechenschaftspflicht

68. Wie bereits in den Nummern 55 und 56 dieser Stellungnahme erläutert, muss auf wirksame Weise sichergestellt werden, dass öffentliche Einrichtungen, die personenbezogene Daten verarbeiten, einer Rechenschaftspflicht unterliegen, und das Abkommen muss Garantien dazu enthalten, wie diese Rechenschaftspflicht durchzusetzen ist. Dies ist umso wichtiger, als im Kontext der Strafverfolgung bei der Verarbeitung personenbezogener Daten generell mangelnde Transparenz herrscht. Unter diesem Aspekt bietet die simple Erwähnung des Umstands, dass die öffentlichen Einrichtungen rechenschaftspflichtig sind, ohne dabei die Modalitäten und Folgen dieser Rechenschaftspflicht näher zu erläutern (dies ist in der Anlage zu dem Bericht der Fall), keine hinreichende Garantie. Der EDSB empfiehlt, entsprechende Erläuterungen in den Wortlaut der Übereinkunft aufzunehmen.

7. Unabhängige und wirksame Beaufsichtigung

69. Der EDSB spricht sich uneingeschränkt für die Aufnahme einer Bestimmung aus, durch die eine unabhängige und wirksame Beaufsichtigung durch eine oder mehrere öffentliche Aufsichtsbehörden sichergestellt wird. Seiner Auffassung nach sollte klargestellt werden, was genau unter der Unabhängigkeit zu verstehen ist, insbesondere, von welchen Stellen die Aufsichtsbehörden unabhängig sind und welchen Stellen sie unterstellt sind. Hierzu sind Kriterien erforderlich, die einer institutionellen und einer funktionalen Unabhängigkeit in Bezug auf die Exekutiv- und Legislativorgane Rechnung tragen. Der EDSB weist darauf hin, dass es sich hierbei um einen wesentlichen Faktor für die Gewährleistung einer wirksamen Einhaltung der vereinbarten Grundsätze handelt. Die Einwirkungs- und Durchsetzungsbefugnisse der Aufsichtsbehörden sind außerdem im Hinblick auf die vorstehend bereits angesprochene Frage der Rechenschaftspflicht der öffentlichen Stellen, die personenbezogene Daten verarbeiten, von entscheidender Bedeutung. Betroffene Personen sollten deutlich auf das Vorhandensein und die Befugnisse der Aufsichtsbehörden hingewiesen werden, damit sie ihre Rechte wahrnehmen können; dies gilt insbesondere dann, wenn je nach dem Kontext der Verarbeitung mehrere Behörden zuständig sind.

70. Darüber hinaus empfiehlt der EDSB, dass in einem künftigen Abkommen auch Mechanismen für eine Zusammenarbeit zwischen den Aufsichtsbehörden vorgesehen werden sollten.

8. Individueller Zugang zu Daten und Berichtigung von Daten

71. Hinsichtlich des Zugangs zu Daten und deren Berichtigung sind im Kontext der Strafverfolgung besondere Garantien erforderlich. Aus diesem Grund begrüßt der EDSB den Grundsatz, dem zufolge Einzelpersonen Zugang zu sie betreffenden personenbezogenen Informationen und das Recht auf „Berichtigung und/oder Streichung" dieser Informationen gewährt wird/gewährt werden muss. Es besteht jedoch nach wie vor eine gewisse Unsicherheit hinsichtlich des Begriffs der Einzelperson (alle betroffenen Personen müssen geschützt werden, nicht nur die Bürger des betreffenden Staates) und hinsichtlich der Bedingungen, unter denen Einzelpersonen Einspruch gegen die Verarbeitung von sie betreffenden Informationen einlegen können. Es muss eindeutiger festgelegt werden, welches die

([23]) Das Abkommen tritt sieben Jahre nach seiner Unterzeichnung außer Kraft und verliert seine Gültigkeit, es sei denn, die Vertragsparteien vereinbaren gegenseitig, das Abkommen zu ersetzen.

„geeigneten Fälle“ sind, in denen Einspruch eingelegt oder nicht eingelegt werden kann. Es sollte für betroffene Personen deutlich sein, unter welchen Umständen — abhängig beispielsweise von der Art der Behörde, der Art der Ermittlungen oder von anderen Kriterien — sie ihre Rechte ausüben können.

72. Überdies sollte für den Fall, dass aus gerechtfertigten Gründen keine direkte Möglichkeit besteht, gegen die Verarbeitung Einspruch einzulegen, eine Möglichkeit zur indirekten Überprüfung bestehen, wobei diese indirekte Überprüfung durch die Behörde vorgenommen werden sollte, die für die Beaufsichtigung der Verarbeitung zuständig ist.

9. Transparenz und Benachrichtigung

73. Der EDSB weist einmal mehr darauf hin, wie wichtig tatsächliche Transparenz dafür ist, dass Einzelpersonen ihre Rechte wahrzunehmen können. Außerdem wird durch tatsächliche Transparenz zur allgemeinen Rechenschaftspflicht öffentlicher Behörden, die personenbezogene Daten verarbeiten, beigetragen. Der EDSB befürwortet diesen Grundsatz in der vorgeschlagenen Form und hebt insbesondere hervor, dass eine allgemeine Benachrichtigung *und* eine individuelle Benachrichtigung der betroffenen Einzelpersonen notwendig ist. In dem in Nummer 9 der Anlage zu dem Bericht enthaltenen Grundsatz-Entwurf wird diesem Umstand Rechnung getragen.

74. In dem Bericht heißt es jedoch in Kapitel 2 Abschnitt A Buchstabe B („Agreed upon Principles“ — Vereinbarte Grundsätze), dass in den Vereinigten Staaten der Begriff Transparenz — einzeln oder in Kombination — die Veröffentlichung im Federal Register, die individuelle Benachrichtigung oder die Offenlegung im Rahmen eines Gerichtsverfahrens umfassen kann. Es muss klar festgeschrieben sein, dass die Veröffentlichung in einem Amtsblatt an sich noch nicht ausreichend ist, um sicherzustellen, dass eine betroffene Person angemessen benachrichtigt wurde. Der EDSB weist darauf hin, dass nicht nur die Notwendigkeit einer individuellen Benachrichtigung besteht, sondern dass darüber hinaus diese Benachrichtigung außerdem in einer Form und in Formulierungen erfolgen muss, die der betroffenen Person leicht verständlich sind.

10. Rechtsbehelf

75. Damit eine Einzelperson ihre Rechte wirksam ausüben kann, muss sie die Möglichkeit haben, Beschwerde bei einer unabhängigen Datenschutzbehörde zu erheben und Rechtsmittel bei einem unabhängigen und unparteiischen Gericht einzulegen. Beide Arten des Rechtsbehelfs sollten gleichermaßen zur Verfügung stehen.

76. Die Möglichkeit der Anrufung einer unabhängigen Datenschutzbehörde muss gegeben sein, da hierdurch in einem Kontext, der Einzelpersonen oftmals sehr undurchsichtig erscheinen mag (nämlich der Kontext der Strafverfolgung), auf flexible und weniger kostspielige Weise Unterstützung gewährt werden kann. Datenschutzbehörden können überdies auch dadurch Unterstützung leisten, dass sie im Namen betroffener Personen deren Recht auf Zugang zu den diese Personen betreffenden personenbezogenen Daten wahrnehmen, wenn diesen Personen aufgrund von Ausnahmeregelungen der Zugang verwehrt wird.

77. Der Zugang zur Gerichtsbarkeit ist eine weitere unerlässliche Garantie dafür, dass betroffene Personen Rechtsbehelf bei einer Behörde einlegen können, die einem anderen Teil des demokratischen Systems angehört als die öffentlichen Einrichtungen, die mit der Verarbeitung der diese Personen betreffenden Daten befasst sind. Eine solche Möglichkeit der wirksamen Anfechtung vor Gericht hält der Europäische Gerichtshof [24] für „wesentlich“ für „die Gewährung eines effektiven Rechtsschutzes. (…) [Dies] stellt […] einen allgemeinen Grundsatz des Gemeinschaftsrechts dar, der sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten ergibt und in den Artikeln 6 und 13 der Europäischen Menschenrechtskonvention verankert ist.“ Das Recht auf einen wirksamen Rechtsbehelf ist außerdem ausdrücklich in Artikel 47 der Charta der Grundrechte der Europäischen Union sowie in Artikel 22 der Richtlinie 95/46 EG verankert, unbeschadet etwaiger Rechtsbehelfe auf Verwaltungsebene.

11. Automatisierte Einzelentscheidungen

78. Der EDSB begrüßt, dass eine Bestimmung vorgesehen ist, durch die für geeignete Garantien bei der automatisierten Verarbeitung personenbezogener Informationen gesorgt wird. Er stellt fest, dass eine gemeinsame Auffassung in der Frage, was als „bedeutende nachteilige Maßnahmen gegen die relevanten Interessen einer Einzelperson“ einzustufen ist, dazu beitragen würde, die Bedingungen für die Anwendung dieses Grundsatzes eindeutig festzulegen.

12. Weiterübermittlung von Daten

79. Die Bedingungen, die für die Weiterübermittlung von Daten gelten, sind nicht in allen Fällen eindeutig festgeschrieben. Dies gilt insbesondere für Fälle, in denen die Weiterübermittlung im Einklang mit internationalen Regelungen und Abkommen zwischen dem übermittelnden und dem empfangenden Staat erfolgen muss: hier sollte konkret angegeben werden, ob auf Abkommen Bezug genommen wird, die zwischen den beiden Staaten geschlossen wurden, die die erste ursprüngliche Datenübermittlung eingeleitet haben, oder auf Abkommen zwischen den beiden Staaten, die an der Weiterübermittlung von Daten beteiligt sind. Der EDSB ist der Auffassung, dass in jedem Fall Abkommen zwischen den beiden Staaten, die die erste ursprüngliche Datenübermittlung eingeleitet haben, bestehen müssen.

80. Der EDSB weist außerdem darauf hin, dass der Begriff des „legitimen öffentlichen Interesses“, dessen Vorliegen Voraussetzung für die Weiterübermittlung ist, sehr weit gefasst ist. Ferner ist unklar, was unter den Begriff der öffentlichen Sicherheit fällt; im Kontext der Strafverfolgung scheint eine Ausweitung der Datenübermittlung auf Fälle von Ethikverstößen und auf reglementierte Berufe weder gerechtfertigt noch angemessen.

VI. **FAZIT**

81. Der EDSB begrüßt die gemeinsame Arbeit seitens der EU und der US-Regierung im Bereich der Strafverfolgung, in dem der Datenschutz von entscheidender Bedeutung ist. Er möchte dennoch deutlich darauf hinweisen, dass es sich hierbei — insbesondere in Bezug auf den genauen Anwendungsbereich und die Art des Abkommens — um eine komplexe Problemstellung handelt und dass deshalb eine gründliche und eingehende Analyse erforderlich ist.

[24] Rechtssache 222/86 *Johnston*, Slg. I-1986, S. 1651, Rechtssache 222/86 *Heylens*, Slg. I-1987 S. 4097; Rechtssache C-97/*91Borelli*, Slg. I-1992 S. 6313.

Die Auswirkungen einer transatlantischen Übereinkunft zum Datenschutz sollten sorgfältig im Zusammenhang mit dem bestehenden Rechtsrahmen und den Folgen für die Bürgerinnen und Bürger geprüft werden.

82. Der EDSB fordert insbesondere in Bezug auf die nachstehenden Punkte eindeutige Abgrenzungen und konkrete Bestimmungen:

— Präzisierung der Art der Übereinkunft, die rechtsverbindlich sein sollte, damit für hinreichende Rechtssicherheit gesorgt ist;

— gründliche Beurteilung der Angemessenheit auf der Basis der grundlegenden Anforderungen in Bezug auf inhaltliche Aspekte der Regelung ebenso wie in Bezug auf Aspekte der Spezifizität und auf die Aufsichtsaspekte der Regelung. Nach Auffassung des EDSB kann die Angemessenheit der allgemeinen Übereinkunft nur anerkannt werden, wenn diese Übereinkunft im Einzelfall mit angemessenen spezifischen Abkommen einhergeht;

— Eingrenzung des Anwendungsbereichs mit einer eindeutigen gemeinsamen Festlegung der Strafverfolgungszwecke, die mit der Übereinkunft verfolgt werden;

— genaue Festlegung der Modalitäten, nach denen privatwirtschaftliche Stellen in Regelungen zur Datenübermittlung einbezogen werden können;

— Einhaltung des Grundsatzes der Verhältnismäßigkeit, was bedeutet, dass ein Datenaustausch auf Einzelfallbasis erfolgt, sofern eine konkrete Notwendigkeit gegeben ist;

— wirkungsvolle Aufsichtsmechanismen und Rechtsbehelfsregelungen für betroffene Personen, einschließlich administrativer und gerichtlicher Rechtsbehelfe;

— wirksame Maßnahmen, durch die sichergestellt wird, dass alle betroffenen Personen unabhängig von ihrer Staatsangehörigkeit ihre Rechte wahrnehmen können;

— Einbeziehung unabhängiger Datenschutzbehörden, insbesondre in Bezug auf die Aufsicht und auf die Unterstützung der betroffenen Personen.

83. Der EDSB weist nachdrücklich darauf hin, dass jegliche Übereilung bei der Ausarbeitung der Grundsätze vermieden werden sollte, da sie zu Lösungen führen könnte, die nicht zufriedenstellend sind und in Bezug auf den Datenschutz eine Wirkung entfalten können, die im Gegensatz zur gewünschten Wirkung steht. Zum gegenwärtigen Zeitpunkt sollte das weitere Vorgehen deshalb darin bestehen, einen Fahrplan im Hinblick auf eine zu einem späteren Zeitpunkt zu schließende Übereinkunft auszuarbeiten.

84. Überdies fordert der EDSB mehr Transparenz bei der Ausarbeitung der Grundsätze für den Datenschutz. Nur wenn alle interessierten Kreise — und auch das Europäische Parlament — einbezogen werden, kann die Übereinkunft mithilfe einer demokratischen Debatte die erforderliche Unterstützung für die Übereinkunft und ihre Anerkennung erhalten.

Geschehen zu Brüssel am 11. November 2008

Peter HUSTINX

Europäischer Datenschutzbeauftragter