Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens 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 (TFTP II)

(2010/C 355/02)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

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

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere Artikel 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 das dem Europäischen Datenschutzbeauftragten übermittelte Ersuchen um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 zum Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, [2] —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Am 15. Juni 2010 nahm die Kommission einen Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens 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 (TFTP) (im Folgenden „der Vorschlag") an. Der Vorschlag (einschließlich des Texts für den Entwurf eines Abkommens mit den Vereinigten Staaten) wurde dem EDSB zur Konsultation übermittelt. Der EDSB begrüßt diese Konsultation und empfiehlt, einen Hinweis auf die vorliegende Stellungnahme in die Präambel des Vorschlags einzufügen.

2. Der Vorschlag der Kommission erfolgte auf Grund von Änderungen in der Architektur von SWIFT [3], durch die seit dem 1. Januar 2010 garantiert wird, dass die von SWIFT versandten Zahlungsverkehrsdaten, die sich auf den Europäischen Wirtschaftsraum und die Schweiz beziehen, innerhalb der europäischen Zone — als Abgrenzung zur transatlantischen Zone — verbleiben und nicht länger im Betriebszentrum in den Vereinigten Staaten gespiegelt werden.

3. Mit dem aktuellen Vorschlag sieht die Kommission zwischen der EU und den Vereinigten Staaten ein internationales Abkommen vor, das auf Artikel 216 (internationale Abkommen), Artikel 82 (justizielle Zusammenarbeit) und Artikel 87 (polizeiliche Zusammenarbeit) des Vertrags über die Arbeitsweise der Europäischen Union beruht und die Übermittlung von relevanten Zahlungsverkehrsdaten, die für die Zwecke des vom US-Finanzministerium eingesetzten Programms zum Aufspüren der Finanzierung des Terrorismus erforderlich sind, an das US-Finanzministerium erforderlich macht.

4. Insbesondere Bezug nehmend auf den Beschluss des Europäischen Parlaments vom 11. Februar 2010, die Zustimmung zu dem am 30. November 2009 unterzeichneten Interimsabkommen zu verweigern, trägt der neue Entwurf insbesondere den Bedenken hinsichtlich des Schutzes von personenbezogenen Daten, einem Grundrecht, das nach dem Inkrafttreten des Vertrags von Lissabon im Rechtsrahmen der Europäischen Union eine noch größere Bedeutung erlangt hat, Rechnung.

5. Im Vorschlag wird die Bedeutung des Datenschutzes durch eine ausdrückliche Bezugnahme auf die entsprechenden Artikel der Verträge und anderer internationaler Übereinkünfte sowie durch die Anerkennung des Datenschutzes als Grundrecht betont. Allerdings wird nicht die Verwendung von Artikel 16 AEUV als Rechtsgrundlage vorgesehen, ungeachtet der Tatsache, dass in Artikel 1 Absatz 1 des vorgeschlagenen Abkommens betont wird, dass ein auf einem hohen Niveau angesiedelter Datenschutz zu seinen wesentlichen Zielen gehört. Diesbezüglich wiederholt der EDSB, dass dieses Abkommen nicht nur den Austausch personenbezogener Daten, sondern ebenfalls den Schutz dieser Daten betrifft. Aus diesem Grund kommt Artikel 16 AEUV keine geringere Relevanz zu, als den Artikeln 82 und 87 AEUV, die sich auf die Zusammenarbeit im Bereich der Rechtsdurchsetzung beziehen und als Rechtsgrundlage gewählt wurden.

6. Der Vorschlag unterliegt dem in Artikel 218 Absatz 6 AEUV aufgeführten Verfahren. Gemäß diesem Verfahren kann die Kommission lediglich nach Zustimmung des Europäischen Parlaments einen Beschluss über die Genehmigung des Abschlusses eines Abkommens verabschieden. Aus diesem Grund ist dieser Vorschlag ein entscheidender „Testfall" für die Anwendung der neuen Lissabonner Verfahren auf ein internationales Abkommen über den Schutz von personenbezogenen Daten. Durch die Gewährleistung einer zufriedenstellenden Festlegung der Datenschutzprinzipien und Garantien in diesem Abkommen wird der Weg für den Erfolg bei anderen Verhandlungen geebnet.

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] SWIFT ist ein in Belgien ansässiges Unternehmen, das einen globalen Datendienst für Finanzinstitute betreibt. Seit 2001 hat das US-Finanzministerium SWIFT administrative Vorladungen geschickt, um Zugang zu bestimmten, mit dem Zahlungsverkehr in Zusammenhang stehenden personenbezogenen Daten zu erhalten, die auf einem Server auf dem Hoheitsgebiet der Vereinigten Staaten gespiegelt werden.

7. In diesem Zusammenhang unterstreicht der EDSB die Bedeutung der Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den Schutz personenbezogener Daten, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten einschließlich Terrorismus im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ausgetauscht und verarbeitet werden. Der Mandatsentwurf für die Aufnahme dieser Verhandlungen wurde von der Kommission am 26. Mai 2010 verabschiedet. Bei der Präsentation dieses Mandatsentwurfs betonte die Kommission die Notwendigkeit eines tragfähigen Abkommens über den Schutz personenbezogener Daten ([1]).

8. Vor diesem Hintergrund empfiehlt der EDSB, dem aktuellen Vorschlag eine eindeutige Verknüpfung zu den Verhandlungen mit den Vereinigten Staaten über diesen allgemeinen Rechtsrahmen für den transatlantischen Datenschutz hinzuzufügen. Es sollte sichergestellt werden, dass diese Standards ebenso im TFTP-II-Abkommen anwendbar sind. Der EDSB empfiehlt, diese Voraussetzung in das aktuelle Abkommen aufzunehmen bzw. zumindest mit der Regierung der Vereinigten Staaten zu vereinbaren, dass ein mögliches künftiges Abkommen über den Datenschutz den im aktuellen Vorschlag vorgesehenen Austausch einschließt.

9. Schließlich unterstützt der EDSB aktiv die Positionen der Datenschutzgruppe nach Artikel 29 und der Arbeitsgruppe Polizei und Justiz. Unabhängig von den in diesen Positionen angeführten oder anzuführenden Argumenten wird in der vorliegenden Stellungnahme unter Berücksichtigung von zu einem früheren Zeitpunkt vorgebrachten Anmerkungen des EDSB, die sich sowohl auf das Interimsabkommen als auch auf die fortlaufenden Verhandlungen mit den Vereinigten Staaten beziehen, der aktuelle Vorschlag analysiert.

II. PRÜFUNG DES VORSCHLAGS

II.1 Vorschlag enthält einige Verbesserungen

10. Der EDSB erkennt an, dass in diesem Vorschlag im Vergleich zum Interimsabkommen TFTP I bestimmte wesentliche Verbesserungen vorgesehen sind, wie zum Beispiel:

— Der Ausschluss von SEPA-Daten. Der Vorschlag sieht ausdrücklich vor, dass Ersuchen des US-Finanzministeriums keine Daten zum Gegenstand haben sollten, die sich auf den einheitlichen Euro-Zahlungsverkehrsraum beziehen (Artikel 4 Absatz 2 Buchstabe d).

— Die Definition des Terrorismus. In Artikel 2 des Vorschlags erfolgt eine Definition des Terrorismus auf der Grundlage von Artikel 1 des Rahmenbeschlusses 2002/475/JI des Rates ([2]).

11. Ferner werden im Vorschlag, über die Forderungen des Europäischen Parlaments und der Europäischen Datenschutzbehörden hinaus, eine Reihe von Bestimmungen festgelegt (Artikel 14-18), die die Rechte der betroffenen Personen zum Gegenstand haben, wie beispielsweise das Recht auf Information, das Recht auf Auskunft, das Recht auf Berichtigung, Löschung oder Sperrung sowie das Recht auf Entschädigung. Allerdings ist die konkrete Durchsetzbarkeit dieser Bestimmungen und Verfahren, die von Nicht-US-Bürgern bzw. nicht auf dem US-Hoheitsgebiet Ansässigen zu befolgen sind, immer noch nicht eindeutig (siehe Kapitel II Artikel 2 Absatz 3 weiter unten).

II.2 Allerdings sind weitere Verbesserungen erforderlich

12. Der EDSB unterstützt in vollem Umfang die in Artikel 1 Absatz 1 des Vorschlags angeführte uneingeschränkte Achtung der Privatsphäre und des Schutzes personenbezogener Daten. In diesem Zusammenhang weist der EDSB darauf hin, dass immer noch einige offene Fragen zu klären und Schlüsselelemente zu verbessern sind, damit die Bestimmungen des Rechtsrahmens der EU zum Schutz personenbezogener Daten eingehalten werden.

II.2.1 *Ist die angestrebte Verarbeitung personenbezogener Daten tatsächlich erforderlich und angemessen?*

13. Der EDSB ist sich voll und ganz bewusst, dass die Bekämpfung des Terrorismus und der Terrorismusfinanzierung eventuelle Beschränkungen des Rechts auf Schutz personenbezogener Daten sowie der Bestimmungen über das Bankgeheimnis erforderlich macht. Dies erfolgt bereits in einer Reihe von EU-Verträgen, ([3]) in denen verschiedene Maßnahmen zur Bekämpfung einer missbräuchlichen Verwendung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung festgelegt sind. Diese Verträge beinhalten ebenso spezifische Bestimmungen zur Gewährleistung des Informationsaustauschs mit den Behörden von Drittländern sowie Garantien zum Schutz von personenbezogenen Daten, die mit der Richtlinie 95/46/EG übereinstimmen.

14. Darüber hinaus gewährleistet das zwischen der EU und den Vereinigten Staaten bestehende Abkommen über gegenseitige Rechtshilfe ausdrücklich den Austausch von Informationen über Bankkonten und den Zahlungsverkehr zwischen den Strafverfolgungsbehörden und es legt die Voraussetzungen und Beschränkungen für diesen Austausch fest. Auf internationaler Ebene bilden die so genannten Egmont Prinzipien ([4]) die Grundlage für den internationalen Austausch von Zahlungsverkehrsdaten zwischen den zentralen Meldestellen, während gleichzeitig Beschränkungen und Garantien im Hinblick auf die Verwendung der ausgetauschten Daten festgelegt werden. Darüber hinaus bestehen bereits Verträge über den Datenaustausch zwischen den Vereinigten Staaten, Europol und Eurojust und gewähren gleichzeitig den Informationsaustausch sowie den Schutz von personenbezogenen Daten.

([1]) Siehe Pressemitteilung: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/609&format=HTML&aged=0&language=EN&guiLanguage=en

([2]) Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung, (ABl. L 164 vom 22.6.2002, S. 3).

([3]) Insbesondere Richtlinie 2005/60/EG zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung sowie Verordnung (EG) Nr. 1781/2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers.

([4]) http://www.egmontgroup.org/library/download/5

15. Vor diesem Hintergrund betont der Vorschlag der Kommission die Geeignetheit des TFTP-Programms, wie er vom US-Finanzministerium und in den Berichten der hochgestellten Persönlichkeit dargelegt wird. Allerdings handelt es sich bei der in Artikel 8 EMRK festgelegten Bestimmung zur Rechtfertigung von Eingriffen in das Privatleben eher um eine „Notwendigkeit" als um eine „Geeignetheit".

16. Nach Ansicht des EDSB muss die tatsächliche Notwendigkeit dieses Abkommens, unter Berücksichtigung bereits bestehender Verträge, ausreichend nachgewiesen werden, oder mit anderen Worten, es ist zu prüfen, inwiefern das Abkommen tatsächlich erforderlich ist, um Ergebnisse zu erzielen, die nicht durch den Einsatz von Verträgen, die einen geringeren Eingriff in die Privatsphäre mit sich bringen, wie beispielsweise die bereits im Rechtsrahmen der EU sowie dem internationalen Rechtsrahmen existierenden Verträge, erreicht werden könnten. Nach Ansicht des EDSB sollte diese zusätzliche Notwendigkeit als Voraussetzung für jedwede Abkommen mit den Vereinigten Staaten über den Austausch von Finanzdaten sowie ebenso angesichts des stark in die Privatsphäre eingreifenden Charakters des Abkommens (siehe ebenfalls die Artikel 18-22 im Hinblick auf die Verhältnismäßigkeit) unmissverständlich dargelegt werden.

17. Der EDSB ist nicht in der Lage, die Notwendigkeit dieses Abkommens zu beurteilen. Allerdings verdienen, selbst wenn die Notwendigkeit des Abkommens erwiesen werden sollte, immer noch andere Punkte die Aufmerksamkeit der Verhandlungsführer.

18. Die Verhältnismäßigkeit ist bei der Beurteilung des Umfangs von übermittelten personenbezogenen Daten und des Aufbewahrungszeitraums für diese Daten ebenfalls das Hauptkriterium. Artikel 4 des Vorschlags beschränkt den Umfang der von den Vereinigten Staaten unterbreitbaren Ersuchen. Allerdings ist im Vorschlag immer noch vorgesehen, personenbezogene Daten in Massenübertragungen an die Vereinigten Staaten zu übermitteln und diese dort während eines Zeitraums von 5 Jahren aufzubewahren, unabhängig davon, ob die Daten extrahiert wurden oder ob eine nachgewiesene Verbindung zu einer bestimmten Ermittlung oder Verfolgung besteht.

Massenübertragungen

19. Der Vorschlag basiert ungeachtet der Forderungen des Europäischen Parlaments sowie der Europäischen Datenschutzbehörden immer noch auf dem Konzept von Massenübertragungen personenbezogener Daten an das US-Finanzministerium. Diesbezüglich ist es wichtig klarzustellen, dass die Tatsache, dass im aktuellen SWIFT-System keine gezielte Suche möglich ist, nicht als eine ausreichende Begründung für die Durchführung von Massenübertragungen von Daten nach dem europäischen Datenschutzrecht angesehen werden kann.

20. Demzufolge ist der EDSB der Ansicht, dass Lösungen gefunden werden sollten, mit deren Hilfe sichergestellt wird, dass die Massenübertragungen durch Mechanismen ersetzt werden, die eine Filterung von Zahlungsverkehrsdaten innerhalb der EU ermöglichen und somit gewährleistet wird, dass ausschließlich relevante und erforderliche Daten an die Behörden der Vereinigten Staaten übermittelt werden. Falls diese Lösungen nicht sofort gefunden werden können, sollte im Abkommen auf jeden Fall eine kurze Übergangsperiode festgelegt werden, nach deren Ablauf Massenübertragungen nicht länger zulässig sind.

Aufbewahrungsfrist

21. Im Hinblick auf die Aufbewahrungsfrist ist der EDSB der Ansicht, dass im Vorschlag maximale Aufbewahrungsfristen korrekt festgelegt sind, sowie Mechanismen zur Sicherstellung, dass personenbezogene Daten gelöscht werden, sobald sie nicht mehr erforderlich sind. Allerdings scheinen die Bestimmungen von Artikel 6 des Vorschlags im Hinblick auf nicht extrahierte Daten in die entgegengesetzte Richtung zu gehen. Zunächst ist das Konzept „nicht extrahierter Daten" nicht eindeutig und sollte deswegen erläutert werden. Zweitens sind die Gründe, auf deren Grundlage es erforderlich ist, nicht extrahierte Daten für einen Zeitraum von 5 Jahren aufzubewahren, nicht nachgewiesen.

22. Der EDSB erkennt in vollem Umfang die Notwendigkeit an, sicherzustellen, dass auf personenbezogene Daten, die für eine bestimmte gerichtete Ermittlung oder Verfolgung gegen Terrorismus benötigt werden, soweit erforderlich, zugegriffen werden kann oder diese Daten verarbeitet und aufbewahrt werden können, in bestimmten Fällen auch für einen 5 Jahre überschreitenden Zeitraum, da personenbezogene Daten für lange andauernde Ermittlungen oder Gerichtsverfahren benötigt werden können. Allerdings sollte in der Annahme, dass es sich bei nicht extrahierten Daten um in Massenübertragungen übermittelte Daten handelt, worauf im Zusammenhang mit einer bestimmten Ermittlung oder Verfolgung weder zugegriffen wird, noch diese Daten verwendet wurden, die Aufbewahrungsfrist, während derer diese Daten gespeichert werden können, weiter eingeschränkt werden. In dieser Hinsicht ist es zweckmäßig hervorzuheben, dass das Bundesverfassungsgericht bei der Speicherung von Telekommunikationsdaten den Standpunkt vertritt, dass eine Aufbewahrungsfrist von 6 Monaten bereits sehr lang ist und folglich einer angemessenen Rechtfertigung bedarf ([1]). Das Verfassungsgericht scheint für Daten, die nicht mit irgendeiner bestimmten Ermittlung in Beziehung stehen, einen Zeitraum von maximal 6 Monaten für angemessen zu erachten.

II.2.2 *Gewährleistest der Vorschlag die Aufsicht durch eine Justizbehörde?*

23. Gemäß dem Verhandlungsmandat sollte einer öffentlichen Justizbehörde die Verantwortung zukommen, die Ersuchen vom US-Finanzministerium entgegenzunehmen, ihre Übereinstimmung mit dem Abkommen zu überprüfen und gegebenenfalls beim Anbieter eine Übermittlung der Daten auf der Grundlage eines „Push"-Systems anzufordern. Sowohl das Europäische Parlament als auch der EDSB begrüßten diese Vorgehensweise, die eine grundlegende Garantie — in Übereinstimmung mit den nationalen Verfassungen und Rechtssystemen der Mitgliedstaaten — zur Gewährleistung rechtmäßiger und ausgewogener Datenübermittlungen sowie einer unabhängigen Aufsicht darstellt.

([1]) Urteil vom 2. März 2010.

24. Allerdings wird diese Aufgabe im Vorschlag Europol, einer EU-Einrichtung für die Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität, von denen zwei oder mehr Mitgliedstaaten betroffen sind, übertragen. ([1]) Es ist offenkundig, dass es sich bei Europol um keine Justizbehörde handelt.

25. Darüber hinaus hat Europol ein bestimmtes Interesse am Austausch von personenbezogenen Daten auf der Grundlage des vorgeschlagenen Abkommens. Artikel 10 des Abkommens stattet Europol mit der Befugnis aus, im Rahmen des TFTP relevante Informationen anzufordern, wenn ein Grund für die Annahme besteht, dass eine natürliche oder juristische Person eine Verbindung zu Terrorismus aufweist. Es ist schwierig, diese Befugnis von Europol, die für die Durchführung der Aufgaben von Europol wichtig sein mag und die gute Beziehungen mit dem US-Finanzministerium voraussetzt, mit der Aufgabe von Europol, eine unabhängige Aufsicht zu gewährleisten, zu vereinbaren.

26. Darüber hinaus fragt sich der EDSB, inwiefern der aktuelle Rechtsrahmen — insbesondere ohne eine Änderung der Rechtsgrundlage gemäß dem im Lissaboner Vertrag festgelegten ordentlichen Verfahren — Europol mit den Aufgaben und Befugnissen betraut, ein administratives Ersuchen aus einem Drittland als „rechtsverbindlich" (Artikel 4 Absatz 5) für ein Privatunternehmen einzustufen, wodurch diese „befugt und verpflichtet" wird, diesem Drittland Daten bereitzustellen. In diesem Zusammenhang ist die Anmerkung angebracht, dass beim aktuellen Stand des EU-Rechts nicht offenkundig ist, ob eine Entscheidung von Europol über ein Privatunternehmen einer gerichtlichen Kontrolle durch den Europäischen Gerichtshof unterliegt.

27. Vor diesem Hintergrund wiederholt der EDSB seinen Standpunkt, ebenso mit Blick auf das Verhandlungsmandat und den aktuellen Rechtsrahmen der EU, dass die Aufgabe zur Überprüfung von Ersuchen des US-Finanzministeriums einer öffentlichen Justizbehörde anvertraut werden sollte.

II.2.3 *Verleiht der Vorschlag den betroffenen Personen durchsetzbare Rechte (und Schutz)?*

28. Wie bereits in der Einleitung zu der vorliegenden Stellungnahme erwähnt, werden im Vorschlag eine Reihe von Rechten der betroffenen Personen festgelegt, wie das Recht auf Information, das Recht auf Auskunft, Löschung oder Sperrung sowie das Recht auf Entschädigung. Allerdings ist es einerseits erforderlich, bestimmte Elemente dieser Bestimmungen zu verbessern und andererseits ihre tatsächliche Durchsetzbarkeit zu gewährleisten.

29. Im Hinblick auf das Recht auf Auskunft über die eigenen personenbezogenen Daten sind im Abkommen eine Reihe von Beschränkungen festgelegt. Der EDSB erkennt an, dass insbesondere im Zusammenhang mit der Bekämpfung von Terrorismus Beschränkungen der Rechte der betroffenen Personen vorgenommen werden können, soweit dies erforderlich ist. Allerdings sollte im Vorschlag deutlich werden, dass, während die Offenlegung von personenbezogenen Daten gegenüber einer betroffenen Person unter den in Artikel 15 Absatz 2 erwähnten Umständen sehr wohl beschränkt werden kann, die Offenlegung dieser Informationen gegenüber den europäischen nationalen Datenschutzbehörden in jedem Fall möglich sein sollte, um diesen Behörden die wirksame Erfüllung ihrer Aufsichtspflicht zu ermöglichen. Selbstverständlich sind die Datenschutzbehörden bei der Durchführung ihrer Aufgaben an eine Geheimhaltungspflicht gebunden und gewähren der betroffenen Person keine Einsicht in die Daten, solange die Voraussetzungen für eine Ausnahme fortbestehen.

30. Im Hinblick auf das Recht auf Berichtigung legt Artikel 17 Absatz 2 fest: „Jede Partei unterrichtet, sofern möglich, die andere Partei, wenn sie feststellt, dass sie auf der Grundlage dieses Abkommens wichtige Angaben übermittelt oder von der anderen Partei erhalten hat, die nicht richtig oder nicht verlässlich sind". Der EDSB ist der Ansicht, dass es sich bei der Verpflichtung zur Berichtigung von nicht richtigen oder nicht verlässlichen Daten um eine grundlegende Garantie nicht nur gegenüber der betroffenen Person, sondern auch hinsichtlich der Handlungseffizienz der Strafverfolgungsbehörden handelt. Daher sollten am Datenaustausch beteiligte Behörden Mechanismen einsetzen, durch die eine Berichtigung immer möglich ist und im Vorschlag sollten folglich die Wörter „sofern möglich" gelöscht werden.

31. Das Hauptanliegen des EDSB bezieht sich allerdings auf die konkrete Durchsetzbarkeit dieser Rechte. Einerseits sollte der Vorschlag aus Gründen der Rechtssicherheit und Transparenz detailliert festlegen, welche konkreten Verfahren die betroffenen Personen nutzen können, um die ihnen vom Abkommen zuerkannten Rechte durchzusetzen, und zwar sowohl in der EU als auch in den Vereinigten Staaten.

32. Anderseits ist in Artikel 20 Absatz 1 ausdrücklich und klar festgelegt, dass durch das Abkommen „(…) keinerlei Rechte oder Vergünstigungen für Personen oder Einrichtungen privater oder öffentlicher Art begründet oder auf diese übertragen ([werden)". Der EDSB merkt an, dass diese Bestimmung den verbindlichen Charakter derjenigen Bestimmungen des Abkommens, durch die unter US-Recht zum aktuellen Zeitpunkt weder anerkannte noch durchsetzbare Rechte der betroffenen Personen gewährleistet werden, zu annullieren oder zumindest in Frage zu stellen scheint, insbesondere wenn es sich bei den betroffenen Personen weder um US-Bürger noch um dauerhaft in den Vereinigten Staaten Ansässige handelt. Beispielsweise gewährt das US-Datenschutzgesetz ein qualifiziertes Recht auf Auskunft über personenbezogene Informationen. Dieses Recht ist dem der Öffentlichkeit durch das US-Gesetz über Informationsfreiheit verliehenen allgemeinen Recht auf Auskunft übergeordnet. Allerdings ist im US-Datenschutz eindeutig festgelegt, dass ein Ersuchen auf Auskunft über sich auf die eigene Person beziehende Informationen ausschließlich möglich ist für „einen Staatsbürger der Vereinigten Staaten oder einen Ausländer, der über eine ordnungsgemäße Aufenthaltserlaubnis verfügt" ([2]).

([1]) Siehe beispielsweise Artikel 3 des Beschlusses 2009/371/JI des Rates zur Errichtung des Europäischen Polizeiamts (Europol), ABl. L 121 vom 15.5.2009, S. 37.

([2]) Dies wird bestätigt durch die Information auf der Website des US-Finanzministeriums: Aus Ihrem Antrag auf Auskunftserteilung sollte hervorgehen, […] dass Sie Staatsbürger der Vereinigten Staaten oder ein Ausländer sind, der über eine ordnungsgemäße Aufenthaltserlaubnis verfügt; […], http://www.treas.gov/foia/how-to.html (letzter Zugriff am 21. Juni 2010).

33. Der EDSB empfiehlt aus diesem Grund, dass die aktuelle Formulierung in Artikel 20 Absatz 1 überarbeitet werden sollte, damit gewährleistet ist, dass die durch den Vorschlag verliehenen Rechte ebenfalls auf dem Hoheitsgebiet der Vereinigten Staaten in deutlicher Form festgelegt und tatsächlich durchsetzbar sind.

II.2.4 *Gewährleistet der Vorschlag eine zufriedenstellende unabhängige Aufsicht und Überwachung?*

34. In Artikel 12 des Vorschlags werden verschiedene Ebenen für die Überwachung der durch das Abkommen festgelegten Bedingungen und Garantien festgelegt. „Unabhängige Prüfer" überwachen in Echtzeit und nachträglich die vom US-Finanzministerium veranlassten Suchabfragen. Darüber hinaus führt „eine unabhängige von der Europäischen Kommission ernannte Person" eine fortlaufende Überwachung der ersten Aufsichtsebene einschließlich deren Unabhängigkeit durch. Es sollte geklärt werden, worin die Aufgabe dieser unabhängigen Person bestehen, wie gewährleistet wird, dass sie ihre Aufgaben effizient erfüllen kann und wem diese Person unterstellt ist.

35. Artikel 13 legt ebenfalls einen Mechanismus für eine gemeinsame Überprüfung fest, die nach 6 Monaten und anschließend in regelmäßigen Abständen durchzuführen ist. Diese gemeinsame Überprüfung wird von einer gemeinsamen EU-US-Delegation durchgeführt, einschließlich Vertretern zweier Datenschutzbehörden für die EU-Delegation, und hat einen Bericht zum Ergebnis, den die Kommission dem Europäischen Parlament und dem Rat vorstellt.

36. Der EDSB betont, dass die unabhängige Überwachung ein Schlüsselelement des Rechts auf den Schutz personenbezogener Daten darstellt, wie von Artikel 16 AEUV und Artikel 8 der Charta der Grundrechte der Europäischen Union bestätigt wird. Vor kurzem hat der Gerichtshof in seinem Urteil vom 9. März 2010 strenge Kriterien für die Unabhängigkeit aufgestellt (Kommission/Bundesrepublik Deutschland) ([1]). Es ist offenkundig, dass Drittländern nicht dieselben strengen Kriterien auferlegt werden können, es ist jedoch ebenfalls klar, dass nur dann ein angemessener Schutz personenbezogener Daten stattfinden kann, ([2]) wenn ausreichende Garantien für eine unabhängige Aufsicht bestehen. Dies ist ebenfalls eine Voraussetzung für internationale Abkommen mit Ländern, deren Rechtssystem nicht die Notwendigkeit einer Kontrolle durch eine unabhängige Behörde vorsieht.

37. Vor diesem Hintergrund ist es von grundlegender Bedeutung, dass im Abkommen zumindest die Modalitäten für die Aufsicht und die gemeinsame Überprüfung sowie die Befugnisse und Unabhängigkeitsgarantien der mit der Aufsicht befassten Personen eindeutig definiert werden, anstatt zu einem späteren Zeitpunkt von den Parteien „gemeinsam koordiniert" oder festgelegt zu werden. Insbesondere ist es wichtig zu gewährleisten, dass sowohl die von der Europäischen Kommission ernannte Person als auch die Vertreter der europäischen Datenschutzbehörden in die Lage versetzt werden, unabhängig zu handeln und ihre Überwachungsaufgaben wirksam durchzuführen.

38. Darüber hinaus sollte im Vorschlag nicht nur der Zeitpunkt für die erste gemeinsame Prüfung festgelegt werden, sondern ebenfalls der Zeitplan für die darauf folgende Überprüfung, die beispielsweise im darauf folgenden Jahr stattfinden könnte. Der EDSB empfiehlt ebenso, eine Beziehung zwischen dem Ergebnis dieser gemeinsamen Überprüfungen und der Dauer des Abkommens zu erstellen.

39. In diesem Zusammenhang betont der EDSB, dass eine Auslaufklausel wünschenswert ist, und zwar ebenso vor dem Hintergrund der möglichen Verfügbarkeit von langfristig stärker zielgerichteten Lösungen. Eine Auslaufklausel könnte ebenfalls als positiver Anreiz zur Gewährleistung dafür dienen, dass die erforderlichen Anstrengungen zur Entwicklung solcher Lösungen in die Wege geleitet werden, wodurch kein Grund zur weiteren Übermittlung von Massendaten an das US-Finanzministerium besteht.

40. Zur Erhöhung der Effizienz sowohl der Aufsicht als auch der gemeinsamen Überprüfung sollten Informationen und relevante Daten zur Anzahl von Ersuchen auf Auskunft und Entschädigung sowie im Hinblick auf die mögliche Weiterbehandlung (Löschung, Berichtigung usw.) verfügbar sein, ebenso, wie zur Anzahl der Entscheidungen über eine Beschränkung der Rechte betroffener Personen. Ebenso sollten im Hinblick auf die Überprüfung Informationen nicht nur hinsichtlich der Anzahl der Zahlungsverkehrsdaten, zu denen das US-Finanzministerium „Zugang" hatte, sondern auch der Zahlungsverkehrsdaten, die dem US-Finanzministerium „bereitgestellt" wurden, verfügbar sein. Dies sollte im Abkommen festgelegt werden.

41. Darüber hinaus sollten die Befugnisse und Zuständigkeiten der europäischen Datenschutzbehörden durch diesen Vorschlag in keiner Weise beschränkt werden. In dieser Hinsicht merkt der EDSB an, dass der Vorschlag im Verhältnis zum TFTP-Interimsabkommen einen Rückschritt bedeutet. Tatsächlich wird in der Präambel des vorhergehenden Abkommens festgelegt, dass „dieses Abkommen keine Abweichung von den bestehenden Befugnissen der Datenschutzbehörden der Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten vorsieht", während im aktuellen Vorschlag nun darauf hingewiesen wird, dass „die bezeichneten Anbieter … unter der Aufsicht der zuständigen Datenschutzbehörden in einer Weise gebunden sind, die mit den besonderen Bestimmungen dieses Abkommens im Einklang steht". Der EDSB empfiehlt aus diesem Grund, im Vorschlag klarzustellen, dass durch das Abkommen die Befugnisse der europäischen Datenschutzbehörden nicht beeinträchtigt oder beschränkt werden.

III. **SCHLUSSFOLGERUNGEN**

42. Der EDSB erkennt an, dass der vorliegende Vorschlag bestimmte wesentliche Verbesserungen im Vergleich zum TFTP I Interimsvertrag beinhaltet, wie beispielsweise den Ausschluss der SEPA-Daten, eine engere Definition des Terrorismus und weitere detaillierte Bestimmungen zu den Rechten der betroffenen Personen.

([1]) Rechtssache C-518/07, noch nicht in der amtlichen Sammlung veröffentlicht.

([2]) In Artikel 8 des vorgeschlagenen Abkommens wird ausgeführt, dass davon ausgegangen wird, dass das US-Finanzministerium einen angemessenen Datenschutz gewährleistet.

43. Der EDSB stellt jedoch fest, dass eine wesentliche Voraussetzung für die Beurteilung der Legitimität eines neuen TFTP-Abkommens eingehalten werden sollte. Die Notwendigkeit des Vertrags muss im Verhältnis zu den bereits bestehenden EU- und internationalen Instrumenten nachgewiesen werden.

44. Sollte dies der Fall sein, weist der EDSB darauf hin, dass immer noch einige offene Fragen zu klären und Schlüsselelemente zu verbessern sind, damit die Bestimmungen des Rechtsrahmens der EU zum Schutz personenbezogener Daten eingehalten werden.

— Gewährleistung, dass Massenübertragungen durch Mechanismen ersetzt werden, in deren Rahmen die Zahlungsverkehrsdaten innerhalb der EU gefiltert werden und Sicherstellung, dass ausschließlich relevante und erforderliche Daten an US-Behörden übermittelt werden;

— Erhebliche Verkürzung der Aufbewahrungsfrist für nicht extrahierte Daten;

— Beauftragung einer öffentlichen Justizbehörde mit der Überprüfung der Ersuchen des US-Finanzministeriums, ebenso mit der Überprüfung des Verhandlungsmandats und des aktuellen EU-Rechtsrahmens;

— Gewährleistung, dass die vom Vorschlag verliehenen Rechte der betroffenen Personen eindeutig festgelegt und ebenso auf dem Hoheitsgebiet der Vereinigten Staaten tatsächlich durchsetzbar sind;

— Verbesserung des Mechanismus zur unabhängigen Aufsicht und Überwachung durch die folgenden Schritte:

i) Gewährleistung, dass die Aufgaben und die Rolle sowohl der von der Europäischen Kommission ernannten Person als auch der Vertreter der europäischen Datenschutzbehörden klar definiert sind und diese in die Lage versetzt werden, unabhängig zu handeln und ihre Überwachungsaufgaben wirksam durchzuführen;

ii) Gewährleistung, dass gemeinsame Überprüfungen regelmäßig durchgeführt werden und dass ihr Ergebnis durch eine Auslaufklausel mit der Dauer des Abkommens verknüpft wird;

iii) Erweiterung der für unabhängige Aufsichtspersonen und Datenschutzbehörden zugänglichen Informationen;

iv) Verhinderung, dass durch das Abkommen die Befugnisse der europäischen Datenschutzbehörden beschränkt werden.

— Einschluss eines Hinweises auf die vorliegende Stellungnahme in die Präambel des Vorschlags.

Geschehen zu Brüssel am 22. Juni 2010.

Peter HUSTINX

Europäischer Datenschutzbeauftragter