Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament und den Rat — „EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa“

(2011/C 101/02)

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 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1],

gestützt auf das dem Europäischen Datenschutzbeauftragten übermittelte Ersuchen um Stellungnahme gemäß 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], insbesondere Artikel 41,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Am 22. November 2010 nahm die Kommission eine Mitteilung mit dem Titel „EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa“ (nachfolgend als „Mitteilung“ bezeichnet) an [3]. Die Mitteilung wurde dem EDSB zur Konsultation zugesandt.

2. Der EDSB begrüßt den Umstand, dass er von der Kommission konsultiert wurde. Er stellte bereits vor der Annahme der Mitteilung informelle Kommentare zum Textentwurf bereit, von denen einige in der endgültigen Fassung der Mitteilung berücksichtigt wurden.

Kontext der Mitteilung

3. Die in der Mitteilung behandelte EU-Strategie der inneren Sicherheit (nachfolgend als ISS bezeichnet) wurde am 23. Februar 2010 unter spanischem Ratsvorsitz angenommen [4]. Die Strategie stellt ein europäisches Sicherheitsmodell vor, in dem — unter Wahrung gemeinsamer europäischer Werte wie der Grundrechte — unter anderem die Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Justizbehörden, dem Grenzschutz und Zivilschutz integriert ist. Die zentralen Ziele der Mitteilung sind:

   — der Öffentlichkeit die bestehenden EU-Instrumente, die bereits zur Gewährung der Sicherheit und Freiheit der EU-Bürger beitragen, sowie den zusätzlichen Nutzen der EU-Tätigkeiten in diesem Bereich vorstellen;

   — gemeinsame Instrumente und Politiken weiterentwickeln, indem ein stärker integrierter Ansatz verwendet wird, in dessen Rahmen die Ursachen der Unsicherheit und nicht nur deren Auswirkungen behandelt werden;

   — die Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Justizbehörden, dem Grenzschutz, dem Zivilschutz und dem Katastrophenschutz stärken.

4. Die ISS zielt darauf ab, die akutesten Bedrohungen und Herausforderungen für die Sicherheit in der EU, wie schwere und organisierte Kriminalität, Terrorismus und Cyberkriminalität, eine bessere Sicherung der Außengrenzen und eine Stärkung der Widerstandsfähigkeit gegenüber natürlichen und vom Menschen verursachten Katastrophen anzugehen. Die Strategie legt allgemeine Leitlinien, Grundsätze und Richtungen fest und gibt vor, wie die EU auf diese Bedrohungen reagieren sollte. Die Kommission wird aufgefordert, zeitlich festgelegte Maßnahmen zur Umsetzung der Strategie vorzuschlagen.

5. Darüber hinaus ist es wichtig, in diesem Zusammenhang auf die jüngsten Schlussfolgerungen des Rats (Justiz und Inneres) zur Schaffung und Umsetzung eines EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität hinzuweisen, die am 8-9. November 2010 [5] (nachfolgend als „Schlussfolgerungen vom November 2010“ bezeichnet) verabschiedet wurden. Dieses Dokument folgt den Schlussfolgerungen des Rates zu der 2006 gebilligten Architektur der Inneren Sicherheit [6] und ruft den Rat und die Kommission dazu auf, eine umfassende ISS auf der Grundlage gemeinsamer EU-Werte und der Grundrechte, die in der EU-Grundrechtecharta erneut bestätigt wurden, festzulegen [7].

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] KOM(2010) 673 endgültig.
[4] Dok. 5842/2/10.
[5] 3043. Tagung des Rates Justiz und Inneres, 8-10. November 2010, Brüssel.
[6] Dok. 7039/2/06 JAI 86 CATS 34.
[7] Der EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität, der im November 2010 thematisiert wurde, besteht aus folgenden vier Schritten: 1) Politikentwicklung auf der Grundlage einer Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der Europäischen Union (EU SOCTA); 2) Politikgestaltung und Beschlussfassung auf der Grundlage einer begrenzten Zahl von Prioritäten, die der Rat ermitteln wird; 3) Durchführung und Überwachung von jährlichen operativen Aktionsplänen (OAP); 4) als Abschluss des Politikzyklus wird eine eingehende Bewertung vorgenommen, die in den nächsten Politikzyklus einfließen wird.

6. Was die Richtlinien und Ziele zur Umsetzung der ISS angeht, verweisen die Schlussfolgerungen vom November 2010 auf Überlegungen zu einer vorausschauenden und auf Erkenntnissen basierenden Vorgehensweise, einer verstärkten Zusammenarbeit zwischen den EU-Agenturen, einschließlich einer weiteren Verbesserung des Informationsaustauschs, sowie dem Ziel, das Bewusstsein der Bürger für die Bedeutung der Arbeit der Union zum Schutz ihrer Bürger zu schärfen. Darüber hinaus wird die Kommission in den Schlussfolgerungen dazu aufgerufen, zusammen mit den Experten der zuständigen Agenturen und der Mitgliedstaaten einen mehrjährigen Strategieplan (MASP) für die jeweiligen Prioritäten zu entwickeln und die am besten geeignete Strategie für eine Problemlösung festzulegen. Die Kommission wird ferner aufgerufen, in Absprache mit den Mitgliedstaaten und EU-Agenturen einen unabhängigen Mechanismus zur Beurteilung der Umsetzung des MASP zu entwickeln. Der EDSB kommt in der vorliegenden Stellungnahme weiter unten auf diese Sachverhalte zurück, da diese eine enge Verbindung zum Schutz personenbezogener Daten, der Privatsphäre und zu anderen hiermit zusammenhängenden grundlegenden Rechten und Freiheiten aufweisen bzw. sich wesentlich auf diese auswirken.

Inhalt und Ziel der Mitteilung

7. In der Mitteilung werden fünf strategische Ziele vorgeschlagen, die alle mit dem Schutz der Privatsphäre und dem Datenschutz verknüpft sind:

   — Schwächung internationaler krimineller Netzwerke,

   — Maßnahmen gegen Terrorismus, Radikalisierung und die Rekrutierung von Terroristen,

   — Besserer Schutz der Bürger und Unternehmen im Cyberspace,

   — Erhöhung der Sicherheit durch Maßnahmen an den Außengrenzen und

   — Verbesserung der Widerstandsfähigkeit Europas gegenüber Krisen und Katastrophen.

8. Die in der Mitteilung vorgeschlagene *ISS* beinhaltet ein gemeinsames Programm für Mitgliedstaaten, das Europäische Parlament, die Kommission, den Rat, die EU-Agenturen und andere Einrichtungen, darunter die Organisationen der Zivilgesellschaft und örtliche Behörden und schlägt vor, wie alle diese Akteure in den nächsten vier Jahren zusammenarbeiten sollten, damit die Ziele der ISS erreicht werden.

9. Die Mitteilung stützt sich auf den Vertrag von Lissabon und erkennt die Leitlinien des Stockholmer Programms (und seines Aktionsplans) an, durch die in Kapitel 4.1 die Notwendigkeit einer umfassenden ISS auf der Grundlage der Achtung der Grundrechte, eines internationalen Schutzes und der Rechtsstaatlichkeit betont wird. Darüber hinaus sollte die Entwicklung, Überwachung und Umsetzung der Strategie der inneren Sicherheit in Übereinstimmung mit dem Stockholmer Programm eine der vorrangigen Aufgaben des nach Maßgabe von Artikel 71 AEUV gegründeten Ständigen Ausschusses für die innere Sicherheit (COSI) werden. Zur Gewährleistung einer wirksamen Durchsetzung der ISS sollten darüber hinaus Sicherheitsaspekte eines integrierten Grenzschutzes sowie gegebenenfalls eine Zusammenarbeit der Justiz in Strafsachen, die für die operative Zusammenarbeit im Bereich der inneren Sicherheit von Bedeutung ist, abgedeckt werden. In diesem Zusammenhang ist auch wichtig zu erwähnen, dass das Stockholmer Programm hinsichtlich der inneren Sicherheit zu einem integrierten Ansatz aufruft, in dessen Rahmen die von der EU entwickelte externe Sicherheitsstrategie sowie andere EU-Strategien ebenfalls berücksichtigt werden, insbesondere diejenigen, die den Binnenmarkt betreffen.

Ziel der Stellungnahme

10. Die Mitteilung bezieht sich auf verschiedene Politikbereiche, die Teil eines breit angelegten Konzepts der „inneren Sicherheit" in der Europäischen Union sind bzw. sich auf dieses auswirken.

11. Das Ziel dieser Stellungnahme besteht nicht in der Analyse aller politischen Bereiche und speziellen Themen, die von der Mitteilung abgedeckt werden, sondern in Folgendem:

   — Untersuchung der in der Mitteilung vorgeschlagenen wesentlichen Ziele der ISS aus der spezifischen Perspektive des Schutzes der Privatsphäre und des Datenschutzes, und — von diesem Blickwinkel aus — Betonung der erforderlichen Verknüpfung mit anderen Strategien, die aktuell auf EU-Ebene diskutiert und verabschiedet werden;

   — Festlegung einer Reihe von Begriffen und Konzepten aus dem Bereich des Datenschutzes, die bei der Gestaltung, Entwicklung und Umsetzung der ISS auf EU-Ebene berücksichtigt werden sollten;

   — sofern dies nützlich und angemessen ist, Bereitstellung von Vorschlägen, inwiefern Datenschutzbelange bei der Umsetzung der in der Mitteilung vorgeschlagenen Maßnahmen am besten berücksichtigt werden können.

12. Der EDSB setzt dies um, indem er insbesondere die Verknüpfungen zwischen der ISS und der Strategie zum Informationsmanagement und der Arbeit an dem umfassenden Datenschutzrahmen betont. Darüber hinaus wird der EDSB auf Konzepte Bezug nehmen wie die besten verfügbaren Methoden und den „eingebauten Datenschutz", die Datenschutzfolgenabschätzung und die Rechte der betroffenen Personen, die sich direkt auf die Gestaltung und die Umsetzung der ISS auswirken. Die Stellungnahme geht ferner auf eine Reihe ausgewählter Politikbereiche ein wie etwa den integrierten Grenzschutz, einschließlich EUROSUR und die Verarbeitung personenbezogener Daten durch FRONTEX, sowie auf andere Bereiche, wie etwa Cyberspace und Programme zum Aufspüren der Finanzierung des Terrorismus.

II. ALLGEMEINE KOMMENTARE

Die Notwendigkeit eines in höherem Maße umfassenden, globalen und „strategischen" Ansatzes bei den mit der ISS verbundenen EU-Strategien

13. Auf EU-Ebene werden zur Zeit verschiedene auf dem Vertrag von Lissabon und dem Stockholmer Programm basierende EU-Strategien mit einer direkten oder indirekten Auswirkung auf den Datenschutz diskutiert und vorgeschlagen. Die ISS ist eine davon und steht in enger Verbindung zu anderen Strategien (die entweder Gegenstand neuerer Mitteilungen der Kommission oder für die nahe Zukunft geplant sind), beispielsweise zu der EU-Strategie zum Informationsmanagement und dem Europäischen Modell zum Informationsaustausch, der Strategie zur Umsetzung der EU-Charta der Grundrechte, der umfassenden Strategie zum Datenschutz und der EU-Politik zur Terrorismusbekämpfung. In der vorliegenden Stellungnahme widmet der EDSB der Verknüpfung mit der Strategie zum Informationsmanagement und dem auf Artikel 16 AEUV basierenden umfassenden Datenschutzrahmen, die aus der Perspektive des Datenschutzes offenkundig strategisch mit der ISS verknüpft sind, besondere Aufmerksamkeit.

14. Alle diese Strategien formen ein komplexes Gebilde von miteinander verbundenen politischen Leitlinien, Programmen und Aktionsplänen, die eine umfassende und integrierte Vorgehensweise auf EU-Ebene erfordern.

15. Allgemein ausgedrückt würde diese Vorgehensweise der „Verknüpfung der Strategien" bei einer Berücksichtigung bei künftigen Aktionen aufzeigen, dass auf EU-Ebene im Hinblick auf die *EU-Strategien* eine Vision vorhanden ist und dass diese Strategien sowie die kürzlich verabschiedeten Mitteilungen über diese Strategien eng miteinander verknüpft sind, was ja tatsächlich der Fall ist, wobei das Stockholmer Programm der Bezugspunkt für alle diese Mitteilungen ist. Dies brächte auch positive Synergien bei verschiedenen Strategien im Raum der Freiheit, der Sicherheit und des Rechts mit sich, und mögliche Überschneidungen von Arbeiten und Bemühungen in diesem Bereich könnten vermieden werden. Ebenso wichtig ist, dass diese Vorgehensweise darüber hinaus zu einer wirksameren und kohärenteren Anwendung der Datenschutzregeln im Kontext sämtlicher miteinander verknüpften Strategien führen würde.

16. Der EDSB betont, dass ein effizientes Informationsmanagement in der Europäischen Union, das auf den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit beruhen sollte, um die Notwendigkeit des Informationsaustauschs zu rechtfertigen, zu den Grundsäulen der ISS gehört.

17. Darüber hinaus unterstreicht der EDSB, wie bereits in seiner Stellungnahme zur Mitteilung über das Informationsmanagement ([8]) erwähnt, dass sämtliche neuen gesetzgeberischen Maßnahmen zur Erleichterung von Speicherung und Austausch personenbezogener Daten lediglich dann vorgeschlagen werden sollten, wenn für deren Notwendigkeit ein konkreter Nachweis erbracht wurde ([9]). Diese rechtliche Anforderung sollte bei der Umsetzung der ISS in eine vorausschauende politische Vorgehensweise umgesetzt werden. Die Notwendigkeit einer umfassenden Vorgehensweise im Hinblick auf die ISS bringt überdies zwangsläufig eine Beurteilung aller im Bereich innere Sicherheit bereits vorhandenen Werkzeuge und Instrumente mit sich, bevor neue vorgeschlagen werden.

18. In diesem Zusammenhang schlägt der EDSB eine häufigere Verwendung von Klauseln zur Gewährleistung einer periodisch erfolgenden Beurteilung bestehender Instrumente vor, wie sie in der aktuell beurteilten Richtlinie zur Datenspeicherung aufgeführt werden ([10]).

Datenschutz als ein Ziel der ISS

19. Die Mitteilung nimmt im Absatz „Sicherheitspolitik auf der Grundlage gemeinsamer Werte" Bezug auf den Schutz personenbezogener Daten. In diesem Absatz wird ausgeführt, dass die Instrumente und Maßnahmen zur Umsetzung der ISS auf gemeinsamen Werten, einschließlich des Grundsatzes der Rechtsstaatlichkeit und der Achtung der Grundrechte, die in der EU-Grundrechtecharta niedergelegt sind, aufbauen müssen. In diesem Zusammenhang wird gefordert: „Werden Informationen zum Zweck der Strafverfolgung in der EU ausgetauscht, müssen wir zudem für den Schutz der Privatsphäre des Einzelnen und seines Grundrechts auf Datenschutz sorgen".

20. Diese Aussage ist begrüßenswert, allerdings kann sie allein nicht als ausreichend für die Auseinandersetzung mit der Frage des Datenschutzes im Rahmen der ISS angesehen werden. Die Mitteilung geht weder auf den Datenschutz näher ein ([11]), noch wird erläutert, wie die Achtung der Privatsphäre und der Schutz personenbezogener Daten in den Maßnahmen zur Umsetzung der ISS praktisch gewährleistet werden sollen.

([8]) Stellungnahme vom 30. September 2010 zur Mitteilung der Kommission an das Europäische Parlament und den Rat — „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht".

([9]) Dies ist eine rechtliche Anforderung, siehe insbesondere das Urteil des EuGH in den verbundenen Rechtssachen C-92/09 und C-93/09 vom 2. November 2010. In spezifischeren Kontexten vertrat der EDSB diese Vorgehensweise auch in anderen Stellungnahmen zu Legislativvorschlägen, die mit dem Raum der Freiheit, der Sicherheit und des Rechts verbunden sind: z. B. in der Stellungnahme vom 19. Oktober 2005 zu drei Vorschlägen im Hinblick auf das Schengener Informationssystem der zweiten Generation (SIS II); in der Stellungnahme vom 20. Dezember 2007 zu dem Entwurf eines Vorschlags für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszecken; in der Stellungnahme vom 18. Februar 2009 zum Vorschlag für eine Verordnung über die Errichtung von „Eurodac" für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EG) Nr. (…/…) (zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist); in der Stellungnahme vom 18. Februar 2009 zu dem Vorschlag zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist, und in der Stellungnahme vom 7. Oktober 2009 zu den Vorschlägen über den Zugang zu EURODAC zu Strafverfolgungszwecken.

([10]) Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, (ABl. L 105 vom 13.4.2006, S. 54).

([11]) Auf den Datenschutz wird lediglich im Zusammenhang mit der Frage der Verarbeitung personenbezogener Daten durch FRONTEX näher eingegangen.

21. Nach Ansicht des EDSB sollte eines der Ziele der *ISS* in einem breit verstandenen *Schutz* bestehen, durch den Ausgewogenheit zwischen dem Schutz der Bürger vor bestehenden Bedrohungen einerseits und dem Schutz ihrer Privatsphäre und ihrem Recht auf Schutz ihrer personenbezogenen Daten andererseits gewährleistet wird. Anders ausgedrückt müssen Bedenken im Hinblick auf die Sicherheit und die Privatsphäre bei der Entwicklung der ISS gleichermaßen ernst genommen werden, was mit dem Stockholmer Programm und den Schlussfolgerungen des Rats im Einklang steht.

22. Kurz gefasst sollte die Gewährleistung der Sicherheit bei einer vollständigen Wahrung des Schutzes der Privatsphäre und des Datenschutzes als ein wesentliches Ziel der EU-Strategie der inneren Sicherheit aufgeführt werden. Dies sollte in allen Maßnahmen, die von den Mitgliedstaaten und EU-Organen zur Umsetzung der Strategie ergriffen werden, zum Ausdruck kommen.

23. In diesem Zusammenhang verweist der EDSB auf die Mitteilung (2010) 609 über ein Gesamtkonzept für den Schutz personenbezogener Daten in der Europäischen Union ([12]). Der EDSB wird demnächst eine Stellungnahme zu dieser Mitteilung abgeben, betont allerdings an dieser Stelle, dass eine effiziente ISS nicht ohne ein solides Datenschutzkonzept umgesetzt werden kann, das die ISS ergänzt und gegenseitiges Vertrauen und eine höhere Wirksamkeit gewährleistet.

III. BEGRIFFE UND KONZEPTE, DIE AUF DIE GESTALTUNG UND DIE UMSETZUNG DER ISS ANZUWENDEN SIND

24. Es ist eindeutig, dass bestimmte Maßnahmen, die aus den Zielen der ISS abgeleitet werden, die Risiken für den Schutz der Privatsphäre und den Datenschutz von Personen erhöhen. Zum Ausgleich dieser Risiken macht der EDSB insbesondere auf Konzepte wie den „eingebauten Datenschutz", die Datenschutzfolgenabschätzung, die Rechte der betroffenen Personen und die besten verfügbaren Methoden aufmerksam. Diese können zu einer stärker die Privatsphäre schützenden und am Datenschutz orientierten Politik in diesem Bereich beitragen und sollten bei der Umsetzung der ISS berücksichtigt werden.

Eingebauter Datenschutz

25. Der EDSB hat bei verschiedenen Anlässen und in verschiedenen Stellungnahmen das Konzept des „eingebauten" Datenschutzes („eingebauter Datenschutz") vertreten. Dieses Konzept wird aktuell sowohl für den privaten als auch für den öffentlichen Sektor entwickelt und muss aus diesem Grund im Zusammenhang mit der inneren Sicherheit der EU und dem Bereich Polizei und Justiz eine wichtige Rolle spielen ([13]).

26. In der Mitteilung wird dieses Konzept nicht erwähnt. Der EDSB empfiehlt, dass auf dieses Konzept in den Maßnahmen, die zur Umsetzung der ISS vorgeschlagen und durchgeführt werden, hingewiesen wird, und zwar insbesondere im Zusammenhang mit Ziel 4, „Erhöhung der Sicherheit durch Maßnahmen an den Außengrenzen", wo eindeutig auf den Einsatz von neuen Technologien für die Grenzkontrolle und die Grenzüberwachung Bezug genommen wird.

Datenschutzfolgenabschätzung

27. Der EDSB fordert die Kommission auf, zu überdenken, was — als Teil der künftigen Arbeit an der Gestaltung und Umsetzung der ISS auf der Grundlage der Mitteilung — mit einer tatsächlichen „Datenschutzfolgenabschätzung" im Raum der Freiheit, der Sicherheit und des Rechts und insbesondere im Rahmen der ISS gemeint ist.

28. Die Mitteilung bezieht sich auf die Beurteilung von Bedrohungen und Risiken. Dies ist begrüßenswert. Allerdings wird hier in keiner Weise auf die Datenschutzfolgenabschätzung Bezug genommen. Der EDSB ist der Ansicht, dass die Arbeit zur Umsetzung der Mitteilung zur ISS eine gute Gelegenheit bietet, um eine solche Datenschutzfolgenabschätzung im Zusammenhang mit der inneren Sicherheit auszuarbeiten. Der EDSB nimmt zur Kenntnis, dass weder die Mitteilung noch die Leitlinien der Kommission zur Folgenabschätzung ([14]) diesen Aspekt festlegen und ihn zu einer Anforderung für die Politik erheben.

29. Aus diesem Grund empfiehlt der EDSB, dass die Kommission bei der Umsetzung von künftigen Instrumenten eine stärker ins Detail gehende und strengere Datenschutzfolgenabschätzung durchführt, sei es als separate Beurteilung oder als Bestandteil einer Folgenabschätzung für die allgemeinen Grundrechte. Diese Folgenabschätzung sollte nicht nur allgemeine Prinzipien aufführen oder politische Möglichkeiten analysieren, wie dies aktuell geschieht, sondern auch spezifische und konkrete Garantien empfehlen.

30. Folglich sollten spezifische Indikatoren und Merkmale entwickelt werden, mit deren Hilfe gewährleistet wird, dass jeder Vorschlag mit einer Auswirkung auf die Privatsphäre und den Datenschutz im Bereich der inneren Sicherheit der EU einer sorgfältigen Abwägung unterzogen wird, einschließlich von Aspekten wie der Verhältnismäßigkeit, der Notwendigkeit und dem Grundsatz der Zweckbindung.

31. Darüber hinaus könnte es in diesem Zusammenhang hilfreich sein, sich auf Artikel 4 der RFID-Empfehlung ([15]) zu beziehen, in der die Kommission die Mitgliedstaaten dazu aufruft, zu gewährleisten, dass die Industrie in Zusammenarbeit mit den entsprechenden Interessenvertretern der Zivilgesellschaft einen Rahmen für eine Datenschutzfolgenabschätzung entwickelt. Darüber hinaus wurde in der im

([12]) Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über ein Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609.

([13]) In seiner Stellungnahme zu der Mitteilung der Kommission über das Stockholmer Programm empfahl der EDSB, dass die Hersteller und Nutzer von Informationssystemen rechtlich dazu verpflichtet werden sollten, mit dem Grundsatz des „eingebauten Datenschutzes" übereinstimmende Systeme zu entwickeln und zu nutzen.

([14]) SEK(2009) 92, 15.1.2009.

([15]) K(2009) 3200 endgültig, 12.5.2009.

November 2009 von der internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre angenommenen Entschließung zu einer Durchführung von Datenschutzfolgenabschätzungen aufgefordert, bevor neue Informationssysteme und Technologien für die Verarbeitung personenbezogener Daten eingeführt oder wesentliche Veränderungen an bestehenden Verarbeitungen vorgenommen werden.

Rechte der betroffenen Personen

32. Der EDSB stellt fest, dass in der Mitteilung die Rechte der betroffenen Personen, die ein grundlegendes Element des Datenschutzes darstellen und sich auf die Gestaltung der ISS auswirken sollten, nicht angesprochen werden. Die Gewährleistung, dass die betroffenen Personen in Bezug auf sämtliche verschiedenen Systeme und Instrumente, die die innere Sicherheit der EU zum Gegenstand haben, ähnliche Rechte im Hinblick darauf genießen, wie ihre Daten verarbeitet werden, ist von grundlegender Bedeutung.

33. Zahlreiche der in der Mitteilung aufgeführten Systeme legen spezifische Vorschriften für die Rechte der betroffenen Personen fest (wobei auch auf Personenkategorien wie Opfer, mutmaßliche Straftäter oder Migranten abgestellt wird), allerdings bestehen zwischen den Systemen und Instrumenten ohne triftige Gründe große Abweichungen.

34. Aus diesem Grund fordert der EDSB die Kommission auf, die Rechte der betroffenen Personen in der EU im Kontext der ISS und der Strategie zum Informationsmanagement in der nahen Zukunft aufeinander abzustimmen.

35. Besondere Aufmerksamkeit sollte den Rechtsbehelfsverfahren gewidmet werden. Die ISS sollte gewährleisten, dass immer dann, wenn die Rechte von Personen nicht in vollem Umfang geachtet werden, die für die Verarbeitung Verantwortlichen einfach zugängliche, wirksame und erschwingliche Beschwerdeverfahren vorsehen.

Die besten verfügbaren Methoden

36. Die Umsetzung der ISS begründet unweigerlich die Verwendung einer IT-Infrastruktur zur Unterstützung der in der Mitteilung vorgesehenen Maßnahmen. Die besten verfügbaren Methoden können als Gewährleistung für ein ausgewogenes Verhältnis zwischen den Zielen der ISS und der Wahrung der Rechte von Personen betrachtet werden. Der EDSB wiederholt im vorliegenden Kontext die bereits in vorhergehenden Stellungnahmen ([16]) ausgesprochene Empfehlung im Hinblick auf die Notwendigkeit, dass die Kommission zusammen mit Interessenvertretern aus der Industrie konkrete Maßnahmen für die Anwendung der besten verfügbaren Methoden definiert und fördert. Diese Anwendung ist gleichbedeutend mit der wirksamsten und am stärksten fortgeschrittenen Phase im Rahmen der Entwicklung von Maßnahmen und ihrer operativen Methoden, was für die praktische Eignung der entsprechenden Methoden zur Erzielung von Ergebnissen spricht, die auf effiziente Weise und in Übereinstimmung mit den EU-Vorschriften zum Schutz der Privatsphäre und des Datenschutzes konzipiert werden. Diese Vorgehensweise steht in vollkommenem Einklang mit der Vorgehensweise im Hinblick auf den weiter oben erwähnten „eingebauten Datenschutz".

37. Sofern dies relevant und durchführbar ist, sollten Referenzdokumente zu den besten verfügbaren Methoden ausgearbeitet werden, um eine Orientierungshilfe und mehr Rechtssicherheit für die Umsetzung der von der ISS vorgesehenen Maßnahmen in die Praxis zu bieten. Dies könnte auch eine Harmonisierung dieser Maßnahmen in den verschiedenen Mitgliedstaaten fördern. Nicht zuletzt erleichtert die Festlegung von der Privatsphäre und der Sicherheit zuträglichen, besten verfügbaren Methoden die Überwachungsfunktion der Datenschutzbehörden, da diese technische Referenzen erhalten, die den Schutz der Privatsphäre und den Datenschutz gewährleisten und von den für die Verarbeitung Verantwortlichen angenommen wurden.

38. Der EDSB stellt überdies fest, dass eine korrekte Ausrichtung der ISS auf die im siebten Rahmenprogramm für Forschung und technologische Entwicklung sowie im Rahmenprogramm „Sicherheit und Schutz der Freiheitsrechte" bereits durchgeführten Maßnahmen von Bedeutung ist. Eine gemeinsame Vision zur Weiterverfolgung und Bereitstellung der besten verfügbaren Methoden unter Wahrung der Grundrechte ermöglicht eine Innovation des Wissens und der Fertigkeiten, die zum Schutz der Bürger erforderlich sind.

39. Schließlich weist der EDSB auf die Rolle hin, die die Europäische Agentur für Netz- und Informationssicherheit (ENISA) bei der Ausarbeitung der Leitlinien und der Beurteilung der für die Gewährleistung der Integrität und Verfügbarkeit der IT-Systeme erforderlichen Sicherheitsfähigkeiten sowie bei der Förderung dieser besten verfügbaren Methoden spielen kann. Diesbezüglich begrüßt der EDSB die Aufnahme der Agentur als wesentlichen Akteur zur Verbesserung der Fähigkeiten im Hinblick auf die Abwehr von Cyberangriffen und die Bekämpfung der Cyberkriminalität ([17]).

Klarstellung der Akteure und ihrer Rollen

40. In diesem Zusammenhang ist eine zusätzliche Klarstellung bezüglich der Akteure, die Teil der ISS-Architektur sind bzw. zu dieser beitragen, erforderlich. Die Mitteilung nimmt auf verschiedene Akteure und Interessenvertreter Bezug, wie z. B. Bürger, die Justiz, EU-Agenturen, nationale Behörden,

([16]) Stellungnahme des EDSB zu intelligenten Transportsystemen vom Juli 2009 und Stellungnahme des EDSB zur RFID Mitteilung vom Dezember 2007, siehe auch den Jahresbericht 2006 des EDSB, S. 48.

([17]) Der EDSB plant die Annahme einer Stellungnahme zum Rechtsrahmen der ENISA noch im Dezember 2010.

Polizei und Wirtschaft. Die spezifischen Rollen und Kompetenzen dieser Akteure sollten im Rahmen der spezifischen, zur Umsetzung der ISS vorgeschlagenen Maßnahmen deutlicher ausgeführt werden.

IV. SPEZIFISCHE KOMMENTARE ZU MIT DER ISS IN VERBINDUNG STEHENDEN POLITIKBEREICHEN

Integrierter Grenzschutz

41. In der Mitteilung wird ausgeführt, dass es seit dem Inkrafttreten des Vertrags von Lissabon für die EU einfacher geworden ist, Synergien zwischen den verschiedenen Vorgehensweisen bei der Grenzverwaltung im Bereich des Personen- und Warenverkehrs herzustellen. Im Bereich des Personenverkehrs heißt es in der Mitteilung, dass „die EU ihre Strategie für ein integriertes Grenzmanagement gleichzeitig auf die Steuerung der Migration und auf Kriminalitätsbekämpfung ausrichten" kann. Das Dokument sieht den Grenzschutz als potenziell leistungsstarkes Mittel zur Schwächung der schweren und organisierten Kriminalität ([18]).

42. Der EDSB stellt ferner fest, dass in der Mitteilung drei strategische Säulen festgelegt werden: 1) ein verstärkter Einsatz neuer Technologien für Grenzkontrollen (SIS II, VIS, Ein-/Ausreise-Informationssystem und das Registrierungsprogramm für Reisende; 2) ein verstärkter Rückgriff auf neue Technologien zur Grenzüberwachung (europäisches Grenzüberwachungssystem EUROSUR) und 3) eine stärkere Koordinierung der Maßnahmen der Mitgliedstaaten durch FRONTEX.

43. Der EDSB nutzt im Rahmen dieser Stellungnahme die Gelegenheit zur Erinnerung an die Ersuchen, die er in einer Reihe von vorhergehenden Stellungnahmen im Hinblick darauf unterbreitete, eine eindeutige Politik im Hinblick auf das Grenzmanagement — unter vollständiger Wahrung der Datenschutzbestimmungen — auf EU-Ebene zu verfolgen. Der EDSB ist der Ansicht, dass die aktuelle Arbeit im Hinblick auf die ISS und das Informationsmanagement eine sehr günstige Gelegenheit bieten, um konkrete Schritte in Richtung einer kohärenten politischen Vorgehensweise in diesem Bereich zu unternehmen.

44. Der EDSB stellt fest, dass in der Mitteilung nicht nur auf die bestehenden Großsysteme und die Systeme, die eventuell in der nahen Zukunft in Betrieb genommen werden (wie z. B. SIS, SIS II und VIS) Bezug genommen wird, sondern im selben Kontext Systeme erwähnt werden, die von der Kommission in Zukunft vorgeschlagen werden könnten, zu denen allerdings noch kein Beschluss gefasst wurde (z. B. das Registrierungsprogramm für Reisende und das Ein-/Ausreisesystem). In diesem Zusammenhang sei daran erinnert, dass die Ziele und die Rechtmäßigkeit dieser Systeme noch geklärt und nachgewiesen werden müssen, auch vor dem Hintergrund der Ergebnisse der von der Kommission durchgeführten spezifischen Folgenabschätzungen. Sollte dies nicht erfolgen, kann die Mitteilung als eine Vorwegnahme des Prozesses zur Beschlussfassung ausgelegt werden, in der folglich der Umstand nicht berücksichtigt wird, dass der letztendliche Beschluss, ob das Registrierungsprogramm für Reisende und das Ein-/Ausreisesystem in der Europäischen Union eingeführt werden sollten, noch nicht gefasst wurde.

45. Der EDSB empfiehlt aus diesem Grund, bei der künftigen Arbeit zur Umsetzung der ISS solche Vorwegnahmen zu vermeiden. Wie bereits früher erwähnt, sollten Beschlüsse zur Einführung von neuen, in die Privatsphäre eingreifenden Großsystemen lediglich nach Abschluss einer angemessenen Beurteilung sämtlicher bestehenden Systeme unter Beachtung der Notwendigkeit und Verhältnismäßigkeit erfolgen.

EUROSUR

46. In der Mitteilung wird erwähnt, dass die Kommission 2011 als Beitrag zur inneren Sicherheit und zur Kriminalitätsbekämpfung einen Legislativvorschlag für EUROSUR vorlegen wird. Es wird ferner ausgeführt, dass für EUROSUR auf neue Technologien zurückgegriffen werden soll, die im Rahmen von mit EU-Mitteln finanzierten Forschungsprojekten entwickelt wurden, beispielsweise die Satellitentechnik zum Aufspüren und Verfolgen von Zielen an den Seegrenzen, etwa von Schnellbooten, mit denen Drogen in die EU verbracht werden.

47. In diesem Zusammenhang stellt der EDSB fest, dass nicht klar ist, ob — und falls ja, in welchem Umfang — der von der Kommission 2011 vorzulegende Legislativvorschlag zu EUROSUR auch die Verarbeitung personenbezogener Daten im Kontext von EUROSUR vorsieht. Die Kommission hat diesbezüglich in der Mitteilung keine klare Position eingenommen. Diese Frage ist umso bedeutender, als in der Mitteilung eine klare Verbindung zwischen EUROSUR und FRONTEX auf taktischer, operativer und strategischer Ebene hergestellt (siehe die Ausführungen zu FRONTEX weiter unten) und zu einer engen Zusammenarbeit zwischen den beiden Organisationen aufgefordert wird.

Die Verarbeitung personenbezogener Daten durch FRONTEX

48. Der EDSB nahm am 17. Mai 2010 eine Stellungnahme zur Änderung der FRONTEX-Verordnung an ([19]), in der er zu einer echten Debatte und eingehenden Überlegungen zum Datenschutz im Zusammenhang mit der Stärkung der bestehenden Aufgaben und der Gewährung neuer Befugnissen für FRONTEX aufruft.

49. In der Mitteilung wird unter Ziel 4, *Erhöhung der Sicherheit durch Maßnahmen an den Außengrenzen*, auf die Notwendigkeit verwiesen, den Beitrag von FRONTEX an den Außengrenzen zu verstärken. In diesem Zusammenhang wird in der Mitteilung erwähnt, dass die Kommission ausgehend von ihren bisherigen Erfahrungen und angesichts des

([18]) Pressemitteilung über die EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa Memo 10/598.

([19]) Stellungnahme des EDSB vom 17. Mai 2010 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 2007/2004 des Rates zur Errichtung einer Europäischen Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union (FRONTEX).

Gesamtkonzepts der EU auf dem Gebiet des Informationsmanagements der Ansicht ist, dass die Zerschlagung krimineller Vereinigungen ein Stück weit erleichtert werden könnte, wenn FRONTEX in begrenztem Umfang nach Festlegung genauer Vorschriften für die Datenverwaltung die Möglichkeit erhielte, diese Informationen zu verarbeiten und zu nutzen. Dies ist eine neue Vorgehensweise im Vergleich zum Vorschlag der Kommission zur Überarbeitung der aktuell vom Europäischen Parlament und dem Rat diskutierten FRONTEX-Verordnung, die sich über die Verarbeitung personenbezogener Daten in Schweigen hüllt.

50. Vor diesem Hintergrund begrüßt der EDSB den Umstand, dass die Mitteilung Hinweise darauf enthält, unter welchen Voraussetzungen eine solche Verarbeitung sich gegebenenfalls als notwendig erweist (z. B. Risikoanalyse, eine bessere Leistung bei gemeinsamen Operationen oder der Informationsaustausch mit Europol). Insbesondere wird in der Mitteilung erläutert, dass derzeit Informationen über Mitglieder von Schleuserbanden oder Drogenringen — die FRONTEX im Zuge ihrer operativen Arbeit zufallen — nicht für Risikoanalysen oder die gezieltere Planung künftiger gemeinsamer Operationen herangezogen werden dürfen. Überdies erreichen einschlägige Informationen über mögliche Straftäter auch nicht die zuständigen nationalen Behörden oder Europol, die weitere Ermittlungen anstellen könnten.

51. Darüber hinaus stellt der EDSB fest, dass die Mitteilung nicht auf die laufende Diskussion über die Überarbeitung des Rechtsrahmens von FRONTEX eingeht , die sich, wie bereits weiter oben erwähnt, mit dieser Frage zwecks Vorgabe gesetzlicher Lösungen befasst. Überdies kann der Wortlaut der Mitteilung, mit dem die Rolle von FRONTEX im Zusammenhang mit dem Ziel der Zerschlagung krimineller Vereinigungen betont wird, als Erweiterung des Mandats von FRONTEX angesehen werden. Der EDSB empfiehlt, diesen Punkt sowohl bei der Überarbeitung der FRONTEX-Verordnung als auch bei der Umsetzung der ISS zu berücksichtigen.

52. Der EDSB macht ferner auf die Notwendigkeit aufmerksam, zu gewährleisten, dass es nicht zu einer Überschneidung der Aufgaben von Europol und FRONTEX kommt. In diesem Zusammenhang begrüßt der EDSB, dass die Mitteilung erwähnt, dass Überschneidungen in der Arbeit von Frontex und Europol vermieden werden sollten. Allerdings sollte diese Frage sowohl in der überarbeiteten FRONTEX-Verordnung als auch in den Maßnahmen zur Umsetzung der ISS, wo eine enge Zusammenarbeit zwischen FRONTEX und Europol vorgesehen ist, deutlicher ausgeführt werden. Dies ist insbesondere vom Standpunkt der Grundsätze der Zweckbindung und der Datenqualität erforderlich. Diese Anmerkung bezieht sich auch auf die künftige Zusammenarbeit mit Agenturen wie der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) oder dem Europäischen Unterstützungsbüro für Asylfragen.

Einsatz der Biometrie

53. In der Mitteilung wird der aktuell verstärkte Einsatz von biometrischen Daten im Raum der Freiheit, der Sicherheit und des Rechts, einschließlich der IT-Großsysteme der EU und anderer Instrumente zum Grenzschutz, nicht speziell aufgegriffen.

54. Der EDSB nutzt daher diese Gelegenheit, um an seine Empfehlung ([20]) zu erinnern, dass dieses vom Standpunkt des Datenschutzes aus höchst sensible Thema bei der Umsetzung der ISS ernsthafte Berücksichtigung finden muss, insbesondere im Zusammenhang mit dem Grenzschutz.

55. Der EDSB empfiehlt darüber hinaus, hinsichtlich des Einsatzes der Biometrie im Raum der Freiheit, der Sicherheit und des Rechts eine klare und stringente Politik zu verfolgen, und zwar auf der Grundlage einer ernsthaften Evaluierung und Abschätzung der Notwendigkeit eines Einsatzes der Biometrie im Rahmen der ISS von Fall zu Fall unter vollständiger Wahrung solch grundlegender Datenschutzgrundsätze wie der Verhältnismäßigkeit, der Notwendigkeit und der Zweckbindung.

TFTP

56. In der Mitteilung wird angekündigt, dass die Kommission 2011 ein EU-Konzept für die Extraktion und Auswertung von in der EU gespeicherten Finanztransaktionsdaten entwickeln wird. In diesem Zusammenhang weist der EDSB auf seine Stellungnahme vom 22. Juni 2010 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) hin. ([21]) Sämtliche kritischen Anmerkungen in dieser Stellungnahme sind im Zusammenhang mit der vorgesehenen Arbeit an einem EU-Rahmen für Zahlungsverkehrsdaten gleichermaßen gültig und anwendbar. Aus diesem Grund sollten diese Anmerkungen bei den Diskussionen über diesen Sachverhalt berücksichtigt werden. Besondere Aufmerksamkeit sollte der Verhältnismäßigkeit bei der Extraktion und Verarbeitung von großen Datenmengen von Personen, die nicht unter einem Verdacht stehen, gewidmet werden, ebenso wie der Frage einer wirksamen Aufsicht durch unabhängige Behörden und die Justiz.

Schutz der Bürger und Unternehmen im Cyberspace

57. Der EDSB begrüßt die Bedeutung, die in der Mitteilung der Vorbeugung auf EU-Ebene beigemessen wird, und vertritt die Ansicht, dass die Stärkung der Sicherheit der IT-Netze ein wesentlicher Faktor ist, der zu einer gut funktionierenden Informationsgesellschaft beiträgt. Der EDSB unterstützt auch die spezifischen Maßnahmen zur Verbesserung des Reaktionsvermögens gegenüber Cyberangriffen, zur Stärkung der Strafverfolgung und der Justizbehörden und zur Errichtung von Partnerschaften mit der Industrie, durch die Bürger und Unternehmen gestärkt werden. Auch die Rolle der ENISA als Triebkraft für zahlreiche unter diesem Ziel vorgesehene Maßnahmen wird begrüßt.

([20]) Siehe insbesondere die Stellungnahme des EDSB zur Mitteilung über das Informationsmanagement im RFSR in Fußnote 8.

([21]) Stellungnahme des EDSB vom 22. Juni 2010 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).

58. Allerdings werden in der *ISS* im Bereich Cyberspace vorgesehene Maßnahmen im Rahmen der Strafverfolgung nicht behandelt. Es wird nicht darauf eingegangen, inwiefern diese Maßnahmen eine Bedrohung für die Rechte von Personen darstellen können und welche Garantien in diesem Zusammenhang erforderlich sind. Der EDSB ruft zu einer ambitionierteren Herangehensweise an geeignete Garantien auf, die zum Schutz der Grundrechte aller Personen, einschließlich derjenigen, die von Maßnahmen gegen mögliche kriminelle Handlungen in diesem Bereich betroffen sind, auf den Weg gebracht werden sollten.

V. **SCHLUSSFOLGERUNG UND EMPFEHLUNGEN**

59. Der EDSB fordert eine Verknüpfung der verschiedenen EU-Strategien und Mitteilungen bei der Umsetzung der ISS. Dieser Vorgehensweise sollte ein konkreter Aktionsplan folgen, der durch eine reale Beurteilung des Bedarfs unterstützt wird. Das Ergebnis sollte eine umfassende, integrierte und gut strukturierte EU-Politik zur ISS sein.

60. Der EDSB ergreift diese Gelegenheit und betont die Bedeutung des rechtlichen Erfordernisses einer Beurteilung sämtlicher bestehenden Instrumente, die im Zusammenhang mit der ISS und dem Informationsaustausch verwendet werden sollen, bevor neue vorgeschlagen werden. In diesem Zusammenhang wird die Aufnahme von Bestimmungen, die regelmäßige Beurteilungen der Effizienz der entsprechenden Instrumente fordern, nachdrücklich empfohlen.

61. Der EDSB empfiehlt, dass im Rahmen der Vorbereitung des in den Schlussfolgerungen des Rates vom November 2010 geforderten mehrjährigen Strategieplans den fortlaufenden Arbeiten an dem umfassenden Datenschutzrahmen auf der Grundlage von Artikel 16 AEUV und insbesondere der Mitteilung (2009) 609 Rechnung getragen werden.

62. Der EDSB gibt eine Reihe von Empfehlungen zu vom Standpunkt des Datenschutzes aus relevanten Begriffen und Konzepten wie dem eingebauten Datenschutz, der Datenschutzfolgenabschätzung und den besten verfügbaren Methoden, die bei der ISS berücksichtigt werden sollten.

63. Der EDSB empfiehlt, dass bei der Umsetzung von künftigen Instrumenten von der Kommission eine Datenschutzfolgenabschätzung durchgeführt wird, sei es als separate Beurteilung oder als Teil einer Folgenabschätzung für die allgemeinen Grundrechte.

64. Der EDSB fordert die Kommission ferner auf, eine kohärentere und konsistentere Politik hinsichtlich der Voraussetzungen für den Einsatz der Biometrie im Bereich der ISS zu verfolgen und auf EU-Ebene für eine stärkere Abstimmung bei den Rechten der betroffenen Personen zu sorgen.

65. Der EDSB kommentiert abschließend die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Grenzschutz und insbesondere durch FRONTEX sowie im möglichen Zusammenhang mit EUROSUR.

Geschehen zu Brüssel am 17. Dezember 2010.

Peter HUSTINX

Europäischer Datenschutzbeauftragter