Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“

(2009/C 276/02)

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

1. Die Kommission hat am 10. Juni 2009 die Mitteilung an das Europäische Parlament und den Rat mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“ ([1]) angenommen. Der Europäische Datenschutzbeauftragte (EDSB) nimmt hiermit gemäß Artikel 41 der Verordnung (EG) Nr. 45/2001 dazu Stellung.

2. Die Kommission hat den EDSB vor der Annahme der Mitteilung mit Schreiben vom 19. Mai 2009 informell dazu konsultiert. Der EDSB hat daraufhin am 20. Mai 2009 informelle Bemerkungen vorgelegt, um eine Verbesserung des Wortlauts der Mitteilung zu bewirken. Darüber hinaus hat der EDSB einen aktiven Beitrag zum Schreiben der Gruppe „Polizei und Justiz“ vom 14. Januar 2009 ([2]) zum Mehrjahresprogramm im Bereich der Freiheit, der Sicherheit und des Rechts geleistet.

3. In der Mitteilung (Abschnitt 1) wird hervorgehoben, dass die Europäische Union „ein neues Mehrjahresprogramm (benötigt), in dem ausgehend von den erzielten Fortschritten die Konsequenzen aus den bestehenden Schwächen gezogen werden und die Zukunft ambitioniert angegangen wird. Dort müssen die Prioritäten für die kommenden fünf Jahre festgelegt werden.“ Dieses Mehrjahresprogramm (bereits unter der Bezeichnung „Stockholmer Programm“ bekannt) wird das Nachfolgeprogramm zum Tampere-Programm und zum Haager Programm bilden, die beide für den Raum der Freiheit, der Sicherheit und des Rechts wichtige politische Impulse gegeben haben.

4. Die Mitteilung soll die Grundlage für dieses neue Mehrjahresprogramm bilden. Der EDSB stellt in diesem Zusammenhang fest, dass von Mehrjahresprogrammen, die an sich keine verbindlichen Instrumente sind, dennoch eine beachtliche Wirkung auf die von den Organen in den betreffenden Bereichen verfolgte Politik ausgeht, da zahlreiche konkrete Maßnahmen legislativer oder sonstiger Art auf diese Programme zurückgehen.

5. Die Mitteilung selbst muss unter diesem Aspekt betrachtet werden. Sie stellt die nächste Phase der Debatte dar, die in etwa eingesetzt hat, als im Juni 2008 von den sogenannten Zukunftsgruppen, die vom Ratsvorsitz eingesetzt wurden, um Denkanstöße zu entwickeln, die beiden Berichte mit den Titeln „Freiheit, Sicherheit, Schutz der Privatsphäre — Europäische Innenpolitik in einer offenen Welt“ ([3]) und „Lösungsvorschläge für das künftige Programm der EU im Justizbereich“ ([4]) vorgelegt wurden.

II. WICHTIGSTE INHALTLICHE PUNKTE DIESER STELLUNGNAHME

6. Die vorliegende Stellungnahme ist nicht nur eine Reaktion auf die Mitteilung, sie ist gleichzeitig auch ein Beitrag des EDSB zu der allgemeineren Diskussion über die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts, an deren Ende, wie vom schwedischen EU-Vorsitz angekündigt ([5]), ein neues strategisches Arbeitsprogramm (das Stockholmer Programm) stehen muss. In dieser Stellungnahme werden außerdem einige Auswirkungen des möglichen Inkrafttretens des Vertrags von Lissabon angesprochen.

7. In Teil III werden die Hauptgesichtspunkte dieser Stellungnahme dargelegt, in Teil IV schließt eine allgemeine Bewertung der Mitteilung an.

8. In Teil V wird die Frage behandelt, wie angesichts des zunehmenden Austauschs personenbezogener Daten der Notwendigkeit des kontinuierlichen Schutzes von Privatsphäre und personenbezogenen Daten Rechnung getragen werden kann. Hierbei wird dem Abschnitt 2.3 der Mitteilung (Schutz personenbezogener Daten und Schutz der Privatsphäre) und allgemeiner dem Bedarf an weiteren legislativen und sonstigen Maßnahmen zur Verbesserung des rechtlichen Rahmens für den Datenschutz besondere Aufmerksamkeit gewidmet.

([1]) KOM(2009) 262 endgültig (im Folgenden als „Mitteilung“ bezeichnet).

([2]) Nicht veröffentlicht. Die Gruppe „Polizei und Justiz“ wurde von der Europäischen Konferenz der Datenschutzbeauftragten eingesetzt, um die Standpunkte der Konferenz im Bereich der Strafverfolgung auszuarbeiten und in dringenden Fragen im Namen der Konferenz zu handeln.

([3]) Ratsdokument Nr. 11657/08. (im Folgenden als „Bericht zur Innenpolitik“ bezeichnet).

([4]) Ratsdokument Nr. 11549/08 (im Folgenden als „Bericht zur Justizpolitik“ bezeichnet).

([5]) Siehe: The Governments EU Work programme, http://www.regeringen.se

9. In Teil VI werden die Erfordernisse und Möglichkeiten behandelt, die bestehen, wenn die Speicherung und der Austausch von Informationen und der Zugang zu Informationen als Instrumente der Strafverfolgung, oder — um es mit den Worten der Mitteilung auszudrücken — als Instrumente für „ein Europa, das Schutz bietet", eingesetzt werden. Abschnitt 4 der Mitteilung enthält eine Reihe von Zielsetzungen bezüglich des Informationsflusses und der technischen Instrumente, insbesondere in den Abschnitten 4.1.2 (Informationsmanagement), 4.1.3 (Mobilisierung der erforderlichen technischen Instrumente) und 4.2.3.2 (Informationssysteme). Die Entwicklung eines europäischen Informationsmodells (Abschnitt 4.1.2) kann in diesem Kontext als der Vorschlag betrachtet werden, der mit den größten Herausforderungen verbunden ist. Der EDSB befasst sich in dieser Stellungnahme ausführlich mit diesem Vorschlag.

10. In Teil VII wird kurz ein spezielles Thema angesprochen, das im Bereich Freiheit, Sicherheit und Recht für den Datenschutz von Bedeutung ist, nämlich der Zugang der Bürger zur Justiz und der elektronische Rechtsverkehr (E-Justiz).

III. HAUPTGESICHTSPUNKTE DIESER STELLUNGNAHME

11. In dieser Stellungnahme erfolgt die Analyse der Mitteilung hauptsächlich unter dem Blickwinkel der Notwendigkeit des Schutzes der Grundrechte und allgemeiner unter dem Blickwinkel der Zukunft des Raums der Freiheit, der Sicherheit und des Rechts, wie er durch das neue Mehrjahresprogramm gestaltet wird. Außerdem stützt sich die Stellungnahme auf die Beiträge des EDSB zur Weiterentwicklung der Politik der Europäischen Union in diesem Bereich, die er hauptsächlich in seiner beratenden Funktion erbracht hat. Bisher hat der EDSB über dreißig Stellungnahmen und Kommentare zu Initiativen, die mit dem Haager Programm in Zusammenhang stehen, abgegeben; alle diese Stellungnahmen und Kommentare sind auf der Website des EDSB abrufbar.

12. Bei seiner Bewertung der Mitteilung wird der EDSB insbesondere den nachstehenden vier Aspekten Rechnung tragen, die für die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts von Bedeutung sind. Diesen vier Aspekten kommt auch in der Mitteilung eine Schlüsselrolle zu.

13. Der erste Aspekt ist die exponentielle Zunahme digitaler Informationen über Bürger als Ergebnis der sich weiterentwickelnden Information- und Kommunikationstechnologien ([6]). Die Gesellschaft entwickelt sich immer mehr zu dem, was oftmals als „Überwachungsgesellschaft" bezeichnet wird, in der damit zu rechnen ist, dass über jede Transaktion und beinahe jede Bewegung eines jeden Bürgers eine digitale Aufzeichnung erstellt wird. Das sogenannte Internet der Dinge und die sogenannte intelligente Umgebung entwickeln sich aufgrund der Nutzung von RFID-Funketiketten bereits sehr schnell. Es werden verstärkt digitalisierte Merkmale des menschlichen Körpers (biometrische Daten) genutzt. Dies führt zu einer immer stärker vernetzten Welt, in der die für öffentliche Sicherheit zuständigen Behörden auf eine riesige Menge potenziell nützlicher Informationen zugreifen können, was sich unmittelbar auf das Leben betroffener Personen auswirken kann.

14. Der zweite Aspekt ist die Internationalisierung. Zum einen wird im digitalen Zeitalter der Datenaustausch nicht durch die Außengrenzen der Europäischen Union begrenzt, zum anderen besteht in der gesamten Bandbreite der Aktivitäten der EU im Raum der Freiheit, der Sicherheit und des Rechts ein wachsender Bedarf an internationaler Zusammenarbeit: beispielhaft seien hier die Bekämpfung des Terrorismus, die polizeiliche und die justizielle Zusammenarbeit, Ziviljustiz und Grenzkontrolle angeführt.

15. Der dritte Aspekt betrifft die Nutzung von Daten zu Strafverfolgungszwecken: Jüngste Bedrohungen der Gesellschaft, ob in Verbindung mit Terrorismus oder nicht, haben zu (einer Nachfrage nach) mehr Möglichkeiten für die Strafverfolgungsbehörden zur Sammlung, zur Speicherung und zum Austausch personenbezogener Daten geführt. In vielen Fällen ist der private Sektor aktiv beteiligt, wie unter anderem aus der Richtlinie über die Vorratsspeicherung von Daten ([7]) und die verschiedenen Rechtsakte zu den Fluggastdatensätzen (PNR) ([8]) ersichtlich ist.

16. Der vierte Aspekt ist die Freizügigkeit und der freie Verkehr. Die allmähliche Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts macht es erforderlich, die Binnengrenzen abzuschaffen und innerhalb dieses Raums bestehende mögliche Hemmnisse für die Freizügigkeit und den freien Verkehr weiter abzubauen. Durch neue Rechtsakte zu diesem Raum sollten in keinem Fall wieder Hemmnisse aufgebaut werden. Im aktuellen Kontext betrifft dies einerseits den freien Verkehr von Personen und andererseits den freien Verkehr von (personenbezogenen) Daten.

17. Diese vier Aspekte machen deutlich, dass das Umfeld, in dem Informationen genutzt werden, sich rasch verändert. Vor diesem Hintergrund kann kein Zweifel daran bestehen, wie wichtig ein starker Mechanismus für den Schutz der Grundrechte der Bürger und insbesondere für den Schutz der Privatsphäre und für den Datenschutz ist. Deshalb hat der EDSB, wie unter Nummer 11 bereits dargelegt, die Schutznotwendigkeit als den Hauptblickwinkel für seine Analyse gewählt.

([6]) In dem Bericht zur Innenpolitik wird in diesem Zusammenhang sogar die Formulierung „digitales Tsunami" gebraucht.

([7]) 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).

([8]) Siehe beispielsweise das 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), ABl. L 204 vom 4.8.2007, S. 18, und den Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, KOM(2007) 654 endgültig.

IV. **ALLGEMEINE BEWERTUNG**

18. Die Mitteilung und das Stockholmer Programm sollen dazu dienen, die Ziele der EU für die nächsten fünf Jahre zu bestimmen, deren Wirkung sich möglicherweise über einen noch längeren Zeitraum erstrecken wird. Der EDSB stellt fest, dass die Mitteilung „Lissabon-neutral", also so abgefasst ist, dass dem Vertrag von Lissabon keine Rechnung getragen wird. Der EDSB kann voll und ganz nachvollziehen, warum die Kommission diesen Ansatz gewählt hat, er bedauert jedoch gleichzeitig, dass die zusätzlichen Möglichkeiten, die der Vertrag von Lissabon eröffnet, in der Mitteilung nicht voll genutzt werden konnten. In dieser Stellungnahme wird ein stärkerer Akzent auf die Perspektive des Vertrags von Lissabon gesetzt.

19. Die Mitteilung baut auf den Ergebnissen der Maßnahmen auf, die von der EU in den letzen Jahren bezüglich des Raums der Freiheit, der Sicherheit und des Rechts durchgeführt wurden. Diese Ergebnisse können als ereignisgesteuert beschrieben werden, mit einem Schwerpunkt auf Maßnahmen, die eine Erweiterung der Befugnisse der Strafverfolgungsbehörden und einen Eingriff in die Privatsphäre der Bürger bewirken. Dies trifft zweifellos auf die Bereiche zu, in denen personenbezogene Daten intensiv genutzt und ausgetauscht werden und in denen somit der Datenschutz besonders wichtig ist. Die Ergebnisse können deshalb als ereignisgesteuert qualifiziert werden, weil externe Ereignisse wie der 11. September und die Bombenanschläge von Madrid und London als starke Triebkraft für Rechtsetzungsmaßnahmen gewirkt haben. So kann beispielsweise die Übermittlung von Fluggastdaten an die Vereinigten Staaten als Folge des 11. Septembers ([9]) gesehen werden, wohingegen die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten ([10]) eine Folge der Bombenanschläge von London war. Der Schwerpunkt wurde auf Maßnahmen gelegt, die einen größeren Eingriff in das Privatleben der Bürger bewirken, da der EU-Gesetzgeber sich auf Maßnahmen konzentriert hat, durch die die Nutzung und der Austausch von Daten erleichtert wurden, wohingegen Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten weniger dringlich waren. Als wichtigste Datenschutzmaßnahme wurde nach dreijährigen Beratungen im Rat der Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden ([11]) verabschiedet. Das Ergebnis war ein nicht ganz zufriedenstellender Rahmenbeschluss des Rates (siehe nachstehende Nummern 29 und 30).

20. Die Erfahrung der letzten Jahre hat gezeigt, dass die Auswirkungen für die Strafverfolgungsbehörden und für den europäischen Bürger bedacht werden müssen, bevor ein neuer Rechtsakt verabschiedet wird. Hierbei sollten die negativen Auswirkungen auf die Privatsphäre und die Wirksamkeit der Maßnahme unter dem Gesichtspunkt der Strafverfolgung von vornherein angemessen berücksichtigt werden, sobald neue Rechtsakte vorgeschlagen und erörtert werden; beides sollte jedoch auch regelmäßig überprüft werden, nachdem die Rechtsakte bereits umgesetzt wurden. Solche Überlegungen sind auch unbedingt erforderlich, bevor im Rahmen eines neuen Mehrjahresprogramms wichtige Initiativen für die nahe Zukunft eingeleitet werden.

21. Der EDSB ist erfreut darüber, dass in der Mitteilung der Schutz der Grundrechte und insbesondere der Schutz personenbezogener Daten als eine der zentralen Fragen für die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts anerkannt wird. In Abschnitt 2 der Mitteilung wird die EU als ein auf gemeinsamen Werten gründender Raum beschrieben, in dem der Schutz der Grundrechte besonders ausgeprägt ist. Positiv ist auch, dass der Beitritt zur Europäischen Menschenrechtskonvention in der Mitteilung als einer der künftigen Handlungsschwerpunkte — sogar als der erste — genannt wird. Dieser Beitritt ist ein wichtiger Schritt zur Gewährleistung eines harmonischen und kohärenten Systems zum Schutz der Grundrechte. Und nicht zuletzt wird dem Datenschutz in der Mitteilung ein herausragender Platz eingeräumt.

22. Dass diesem Thema in der Mitteilung so viel Raum gewidmet ist, macht deutlich, dass die feste Absicht besteht, die Rechte der Bürger zu schützen und dabei für Ausgewogenheit zu sorgen. Die Regierungen brauchen geeignete Instrumente, um die Sicherheit ihrer Bürger zu garantieren, gleichzeitig müssen sie aber in unserer europäischen Gesellschaft auch die Grundrechte der Bürger uneingeschränkt wahren. Um im Dienste der Bürger ([12]) stehen zu können, muss die Europäische Union hier ein ausgewogenes Verhältnis wahren.

23. Nach Ansicht des EDSB wird in der Mitteilung dieser Notwendigkeit eines ausgewogenen Verhältnisses, einschließlich der Notwendigkeit des Schutzes personenbezogener Daten, auf gute Weise Rechnung getragen. In der Mitteilung wird eingestanden, dass ein anderer Schwerpunkt gesetzt werden muss. Dies ist wichtig, da durch die politischen Maßnahmen, die im Zusammenhang mit dem Raum der Freiheit, der Sicherheit und des Rechts getroffen werden, keinesfalls eine schrittweise Entwicklung hin zu einer Überwachungsgesellschaft gefördert werden soll. Der EDSB hofft, dass der Rat im Stockholmer Programm dem gleichen Ansatz folgen wird, unter anderem, indem er die in Nummer 25 dargelegten Leitgedanken anerkennt.

24. Dies ist umso wichtiger, als der Raum der Freiheit, der Sicherheit und des Rechts ein Bereich ist, der „die Lebensumstände der Bürger, vor allem ihren von den Grundrechten geschützten privaten Raum der Eigenverantwortung und der persönlichen und sozialen Sicherheit prägt", wie das Bundesverfassungsgericht vor Kurzem in seiner Entscheidung vom 30. Juni 2009 zum Vertrag von Lissabon ([13]) feststellte.

([9]) Das PNR-Abkommen von 2007 gemäß Fußnote 8 und seine Vorläufer.

([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). Auch wenn Artikel 95 EGV die Rechtsgrundlage ist, war die Richtlinie dennoch eine unmittelbare Reaktion auf die Bombenanschläge von London.

([11]) Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

([12]) Vgl. den Titel der Mitteilung.

([13]) Bundesverfassungsgericht, Pressemitteilung Nr. 72/2009 vom 30. Juni 2009, Nummer 2 Buchstabe c.

25. Der EDSB hebt hervor, dass für einen solchen Raum der Freiheit, der Sicherheit und des Rechts Folgendes gelten sollte:

— Informationen sollten zwischen den Behörden der Mitgliedstaaten — einschließlich, soweit angebracht, der europäischen Einrichtungen oder Datenbanken — auf der Grundlage geeigneter und wirksamer Mechanismen ausgetauscht werden, durch die die Grundrechte der Bürger uneingeschränkt gewahrt werden und gegenseitiges Vertrauen sichergestellt wird.

— Hierfür ist nicht nur die Verfügbarkeit von Informationen, verbunden mit einer gegenseitigen Anerkennung der Rechtssysteme der Mitgliedstaaten (und der EU), erforderlich, sondern auch eine Harmonisierung der Standards für den Schutz der Informationen, beispielsweise, jedoch nicht ausschließlich, durch einen gemeinsamen rechtlichen Rahmen für den Datenschutz.

— Diese gemeinsamen Standards sollten nicht nur in Fällen mit grenzüberschreitender Dimension anwendbar sein. Gegenseitiges Vertrauen kann nur dann bestehen, wenn die Standards solide sind und stets eingehalten werden, ohne dass die Gefahr besteht, dass sie nicht zur Anwendung kommen, sobald die grenzüberschreitende Dimension nicht oder nicht mehr offensichtlich ist. Abgesehen davon kann — insbesondere wenn es um die Nutzung von Informationen geht — die Unterscheidung zwischen „internen" und „grenzüberschreitenden" Daten in der Praxis nicht aufrechterhalten werden ([14]).

V. INSTRUMENTE FÜR DEN DATENSCHUTZ

V.1 Schaffung einer umfassenden Regelung zum Datenschutz

26. Der EDSB pflichtet der strategischen Überlegung bei, dem Datenschutz in der Mitteilung einen herausragenden Platz einzuräumen. Da zahlreiche Initiativen im Bereich des Raums der Freiheit, der Sicherheit und des Rechts auf der Nutzung personenbezogener Daten beruhen, ist ein guter Datenschutz von entscheidender Bedeutung für den Erfolg dieser Initiativen. Die Achtung der Privatsphäre und der Datenschutz sind nicht nur eine rechtliche Verpflichtung, die auf EU-Ebene immer stärker Anerkennung findet, sondern auch ein zentrales Anliegen der europäischen Bürger, wie die Ergebnisse des Eurobarometers zeigen ([15]). Außerdem ist es auch äußerst wichtig, den Zugang zu personenbezogenen Daten zu begrenzen, um das Vertrauen der Strafverfolgungsbehörden sicherzustellen.

27. In Abschnitt 2.3 der Mitteilung heißt es, dass eine umfassende Regelung zum Datenschutz geschaffen werden muss, die für sämtliche Zuständigkeitsbereiche der EU gleichermaßen gilt ([16]). Der EDSB befürwortet dieses Ziel voll und ganz, unabhängig davon, ob der Vertrag von Lissabon in Kraft tritt oder nicht. Außerdem stellt er fest, dass eine solche Regelung nicht unbedingt bedeuten muss, dass ein einziger rechtlicher Rahmen für die gesamte Datenverarbeitung gilt. Nach den geltenden Verträgen bestehen nur eingeschränkte Möglichkeiten, einen umfassenden rechtlichen Rahmen für die gesamte Datenverarbeitung festzulegen; der Grund hierfür liegt in der Säulenstruktur und darin, dass — zumindest in der ersten Säule — für den Schutz von Daten, die von den europäischen Organen und Einrichtungen verarbeitet werden, eine gesonderte Rechtsgrundlage (Artikel 286 EGV) gilt. Der EDSB weist jedoch darauf hin, dass einige Verbesserungen bereits dadurch erreicht werden könnten, dass die durch die geltenden Verträge gebotenen Möglichkeiten voll ausgenutzt werden, wie die Kommission bereits in ihrer Mitteilung mit dem Titel „Umsetzung des Haager Programms: Weitere Schritte" ([17]) aufgezeigt hat. Nach Inkrafttreten des Vertrags von Lissabon wird Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union die notwendige Rechtsgrundlage für einen umfassenden rechtlichen Rahmen für die gesamte Datenverarbeitung bilden.

28. Der EDSB stellt fest, dass es in jedem Fall äußerst wichtig ist, dass innerhalb des Rechtsrahmens für den Datenschutz für Kohärenz gesorgt wird, nötigenfalls durch Harmonisierung und Konsolidierung der verschiedenen Rechtsakte, die für den Raum der Freiheit, der Sicherheit und des Rechts gelten.

Lage nach den geltenden Verträgen

29. Ein erster Schritt war die jüngst erfolgte Annahme des Rahmenbeschlusses 2008/977/JI des Rates ([18]). Dieser Rechtsakt kann jedoch nicht als umfassender rechtlicher Rahmen betrachtet werden, und zwar im wesentlichen, weil seine Bestimmungen keine umfassende Geltung haben. Sie gelten nicht für innerstaatliche Situationen, in denen personenbezogene Daten von dem Mitgliedstaat stammen, der sie nutzt. Durch diese Einschränkung wird der zusätzliche Nutzen des Rahmenbeschlusses des Rates von vornherein gemindert, es sei denn, alle Mitgliedstaaten würden sich entschließen, die innerstaatlichen Situationen in ihre einzelstaatlichen Ausführungsbestimmungen aufzunehmen, was jedoch nicht sehr wahrscheinlich ist.

30. Der zweite Grund, aus dem nach Auffassung des EDSB der Rahmenbeschluss 2008/977/JI des Rates auf lange Sicht keinen zufriedenstellenden rechtlichen Rahmen für den Datenschutz in einem Raum der Freiheit, der Sicherheit und des Rechts bietet, liegt darin, dass mehrere wesentliche Bestimmungen des Beschlusses nicht mit der Richtlinie 95/46/EG im Einklang stehen. Nach den geltenden Verträgen könnte ein zweiter Schritt darin bestehen, den Geltungsbereich des Rahmenbeschlusses des Rates auszuweiten und ihn an die Richtlinie 95/46/EG anzupassen.

31. Der Schaffung einer umfassenden Regelung zum Datenschutz könnte ein weiterer Impuls dadurch gegeben werden, dass eine klare langfristige Zukunftsprojektion vereinbart wird. Diese Zukunftsprojektion könnte ein umfassendes und schlüssiges Konzept für die Definition von Datenerhebung und Datenaustausch — sowie für den Betrieb

([14]) Der EDSB hat diesen letzten Punkt in seiner Stellungnahme vom 19. Dezember 2005 zu dem *Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden* (KOM(2005) 475 endg.), ABl. C 47 vom 25.2.2006, S. 27, Nummern 30 bis 32, näher ausgeführt.

([15]) Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer Series 225, Jan. 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Siehe auch den Abschnitt der Mitteilung zu den künftigen Handlungsschwerpunkten.

([17]) KOM(2006) 331 endg. vom 28. Juni 2006.

([18]) Siehe Fußnote 11.

bestehender Datenbanken — und gleichzeitig Datenschutzgarantien enthalten. Sie sollte nutzlose Überschneidungen von Rechtsakten und Mehrfachregelungen (und so die Mehrfachverarbeitung personenbezogener Daten) verhindern. Ferner sollte durch sie die Kohärenz der politischen Maßnahmen der EU in diesem Bereich und das Vertrauen darin, wie Behörden mit den Daten der Bürger umgehen, gefördert werden. Der EDSB empfiehlt dem Rat, die Notwendigkeit einer klaren und langfristigen Zukunftsprojektion im Stockholmer Programm zu verankern.

32. Der EDSB empfiehlt außerdem, die in diesem Bereich bereits verabschiedeten Maßnahmen, ihre tatsächliche Durchführung und ihre Wirksamkeit zu bewerten und in die richtige Perspektive zu rücken. Dabei sollten die negativen Auswirkungen auf die Privatsphäre und die Wirksamkeit dieser Maßnahmen für die Strafverfolgung in geeigneter Weise berücksichtigt werden. Sollte die Bewertung ergeben, dass bestimmte Maßnahmen nicht das erwartete Ergebnis erbringen oder für das verfolgte Ziel nicht angemessen sind, so sollten folgende Schritte erwogen werden:

— Als erster Schritt die Änderung oder Aufhebung der Maßnahmen insoweit, als sie sich nicht hinreichend dadurch rechtfertigen lassen, dass sie einen konkreten zusätzlichen Nutzen für die Strafverfolgungsbehörden und den europäischen Bürger bewirken;

— als zweiter Schritt die Bewertung der Möglichkeiten, die Anwendung der bestehenden Maßnahmen zu verbessern;

— und erst als dritter Schritt neue Legislativvorschläge, wenn anzunehmen ist, dass diese für den verfolgten Zweck erforderlich sind. Neue Rechtsakte sollten nur dann verabschiedet werden, wenn sie einen eindeutigen und konkreten zusätzlichen Nutzen für die Strafverfolgungsbehörden und den europäischen Bürger bewirken.

Der EDSB empfiehlt, eine Bezugnahme auf ein System zur Bewertung bestehender Maßnahmen in das Stockholmer Programm aufzunehmen.

33. Nicht zuletzt sollte, entsprechend der Mitteilung der Kommission über den Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie ([19]) und den vom EDSB in seiner Stellungnahme zu dieser Mitteilung ([20]) ausgesprochenen Empfehlungen, ein besonderes Augenmerk auf eine bessere Anwendung der bestehenden Garantien gelegt werden. Bedauerlicherweise hat die Kommission bezüglich der dritten Säule nicht die Möglichkeit, Verletzungsklagen einzuleiten.

Lage nach dem Vertrag von Lissabon

34. Der Vertrag von Lissabon eröffnet die Möglichkeit für einen wirklich umfassenden rechtlichen Rahmen für den Datenschutz. Nach Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union obliegt es dem Rat und dem Europäischen Parlament, Vorschriften über den Datenschutz durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten, soweit diese Tätigkeiten ausüben, die in den Anwendungsbereich des Unionsrechts fallen, sowie über den Datenschutz durch den privaten Sektor zu erlassen.

35. Der EDSB geht davon aus, dass das besondere Augenmerk, das in der Mitteilung auf eine umfassende Regelung zum Datenschutz gelegt wird, Ausdruck des Strebens der Kommission ist, einen rechtlichen Rahmen vorzuschlagen, der auf alle Datenverarbeitungstätigkeiten anwendbar wäre. Er unterstützt dieses Streben voll und ganz, da hierdurch für eine stärkere Kohärenz des Systems und für Rechtssicherheit gesorgt wird und somit eine Verbesserung des Schutzes bewirkt wird. Insbesondere würden hierdurch in Zukunft die Schwierigkeiten vermieden, die auftreten, wenn es darum geht, eine Trennungslinie zwischen den Säulen zu ziehen, wenn Daten, die im privaten Sektor zu Geschäftszwecken erhoben wurden, zu einem späteren Zeitpunkt für Strafverfolgungszwecke genutzt werden. Die Trennungslinie zwischen den Säulen entspricht nicht vollständig der Realität, wie wichtige Urteile des Gerichtshofs in Sachen Fluggastdatensätze ([21]) und Vorratsspeicherung von Daten ([22]) zeigen.

36. Der EDSB schlägt vor, dieses Grundprinzip einer umfassenden Datenschutzregelung in das Stockholmer Programm aufzunehmen. Es verdeutlicht, dass eine solche Regelung nicht einfach nur aus einer Vorliebe heraus geschaffen wird, sondern aufgrund der sich ändernden Praxis der Datennutzung eine Notwendigkeit ist. Der EDSB empfiehlt, die Notwendigkeit eines neuen rechtlichen Rahmens, der unter anderem an die Stelle des Rahmenbeschlusses 2008/977/JI des Rates treten soll, als einen Handlungsschwerpunkt in das Stockholmer Programm aufzunehmen.

37. Der EDSB betont, dass eine umfassende Regelung zum Datenschutz, die sich auf einen allgemeinen rechtlichen Rahmen stützt, nicht ausschließt, dass ergänzende Vorschriften zum Datenschutz im Polizei- und Justizbereich erlassen werden. In diesen ergänzenden Vorschriften könnte den spezifischen Bedürfnissen der Strafverfolgung Rechnung getragen werden, wie es in der Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon ([23]) vorgesehen ist.

V.2 **Neuformulierung der Grundsätze des Datenschutzes**

38. In der Mitteilung wird festgestellt, dass der technische Wandel die Kommunikation zwischen Einzelpersonen und öffentlichen und privaten Einrichtungen verändert. Nach Auffassung der Kommission macht dies eine Neuformulierung einiger grundlegender Prinzipien des Datenschutzes erforderlich.

([19]) KOM(2007) 87 endg. vom 7. März 2007.

([20]) Stellungnahme vom 25. Juli 2007, ABl. C 255 vom 27.10.2007, S. 1, insbesondere Nummer 30.

([21]) 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.

([22]) Urteil des Gerichtshofs vom 10. Februar 2009, Irland gegen Europäisches Parlament und Rat der Europäischen Union, Rechtssache C-301/06; noch nicht archiviert.

([23]) Vgl. Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon angenommen hat, ABl. C 115 vom 9.5.2008, S. 345.

39. Der EDSB begrüßt dieses Bestreben. Vor dem Hintergrund des technischen Wandels ist eine Bewertung der Wirksamkeit der Grundsätze äußerst zweckmäßig. Zunächst einmal muss festgehalten werden, dass die Neuformulierung und die Bekräftigung von Grundsätzen des Datenschutzes nicht immer in direktem Zusammenhang mit technischen Entwicklungen stehen müssen. Sie können sich auch unter anderen Aspekten, nämlich unter den im vorstehenden Teil III aufgeführten Aspekten der Internationalisierung, der vermehrten Nutzung von Daten zu Strafverfolgungszwecken und der Freizügigkeit, als notwendig erweisen.

40. Außerdem kann diese Bewertung nach Auffassung des EDSB in die offene Konsultation eingeschlossen werden, die die Kommission bei der Datenschutzkonferenz mit dem Titel „Personenbezogene Daten — größere Nutzung, größerer Schutz?" vom 19. und 20. Mai 2009 angekündigt hat. Diese offene Konsultation könnte wertvolle Denkanstöße liefern ([24]). Der EDSB schlägt vor, dass der Zusammenhang zwischen den in Abschnitt 2.3 der Mitteilung dargelegten Zielen und der offenen Konsultation zur Zukunft des Datenschutzes vom Rat im Stockholmer Programm und von der Kommission in ihren öffentlichen Erklärungen zu der Konsultation deutlich herausgestellt wird.

41. Die folgenden Punkte sollen veranschaulichen, welche Aspekte durch eine derartige Bewertung abgedeckt werden könnten:

— In den Bereichen Freiheit, Sicherheit und Recht dürfte es sich bei personenbezogenen Daten um besonders sensible Daten handeln, beispielsweise um Daten zu strafrechtlichen Verurteilungen, polizeiliche Daten und biometrische Daten wie Fingerabdrücke und DNA-Profile.

— Die Verarbeitung solcher sensiblen Daten kann für die betroffenen Personen negative Folgen haben, besonders, wenn man bedenkt, dass die Strafverfolgungsbehörden zur Anwendung von Zwangsmaßnahmen befugt sind. Hinzu kommt, dass die Datenüberwachung und -analyse immer stärker automatisiert ist und relativ häufig ohne menschliches Zutun erfolgt. Die Technik ermöglicht die Nutzung von Datenbanken, die personenbezogene Daten enthalten, für allgemeine Suchläufe (Data Mining, Profiling usw.). Die rechtlichen Verpflichtungen, auf deren Grundlage die Datenverarbeitung erfolgt, sollten eindeutig festgelegt werden.

— Ein Dreh- und Angelpunkt der Datenschutzgesetzgebung besteht darin, dass personenbezogene Daten nur für bestimmte festgelegte Zwecke erhoben und nicht zweckwidrig verwendet werden dürfen. Die Verwendung von Daten für andere Zwecke sollte nur insoweit zulässig sein, als dies gesetzlich geregelt und zur Verfolgung spezifischer öffentlicher Interessen, wie sie in Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention festgelegt sind, notwendig ist.

— Die Notwendigkeit der Einhaltung des Grundsatzes der Zweckbindung könnte sich auf die gegenwärtigen Entwicklungen bei der Verwendung von Daten auswirken. Bei der Strafverfolgung werden Daten genutzt, die von privatwirtschaftlichen Unternehmen zu Geschäftszwecken in den Bereichen Telekommunikation und Verkehr und im Finanzsektor erhoben wurden. Hinzu kommt, dass beispielsweise in den Bereichen Einwanderung und Grenzkontrolle groß angelegte Informationssysteme geschaffen werden. Überdies sind Zusammenschaltungen von Datenbanken und der Zugriff auf Datenbanken zulässig, so dass die Daten zu Zwecken verwendet werden können, die weit über den Zweck, zu dem sie ursprünglich erhoben wurden, hinausgehen. Zu diesen gegenwärtigen Entwicklungen müssen Überlegungen angestellt werden, die nötigenfalls die möglichen Anpassungen und/oder zusätzliche Garantien einschließen sollten.

— Bei der Bewertung sollte — ergänzend zu den in der Mitteilung genannten Grundsätzen des Datenschutzes — der Notwendigkeit von Transparenz bei der Verarbeitung Rechnung getragen werden, die es den betroffenen Personen ermöglicht, ihre Rechte wahrzunehmen. Transparenz ist im Bereich der Strafverfolgung ein besonders schwieriges Thema, insbesondere weil hier Transparenz und das Risiko einer Gefährdung der Ermittlungen gegeneinander abgewogen werden müssen.

— Für den Datenaustausch mit Drittstaaten sollten Lösungen gefunden werden.

42. Bei der Bewertung sollte außerdem ein Schwerpunkt auf die Frage gelegt werden, welche Möglichkeiten bestehen, um eine wirksamere Anwendung der Datenschutzgrundsätze zu erreichen. In diesem Zusammenhang könnte es nützlich sein, den Schwerpunkt auf Instrumente zu legen, durch die die Befugnisse der für die Verarbeitung Verantwortlichen erweitert werden können. Diese Instrumente müssen es ermöglichen, dass die volle Verantwortung für das Datenmanagement bei den für die Verarbeitung Verantwortlichen liegt. Data Governance ist in diesem Kontext ein nützlicher Begriff. Er umfasst alle rechtlichen, technischen und organisatorischen Mittel, die es Organisationen erlauben, die volle Verantwortung dafür zu übernehmen, wie Daten verarbeitet werden, nämlich beispielsweise Planung und Kontrolle, Einsatz von sicherer Technik, angemessene Ausbildung des Personals, Prüfung der Einhaltung von Vorschriften usw.

V.3 **Datenschutzfreundliche Technologien**

43. Der EDSB ist erfreut darüber, dass in Abschnitt 2.3 der Mitteilung ein Zertifizierungsverfahren für Datenschutzfreundlichkeit angesprochen wird. Ergänzend dazu könnte auf den „eingebauten Datenschutz" (privacy by design) und auf die Notwendigkeit abgestellt werden, die „besten verfügbaren Techniken" im Einklang mit dem rechtlichen Rahmen der EU für den Datenschutz zu ermitteln.

44. Nach Auffassung des EDSB könnten der „eingebaute Datenschutz" und datenschutzfreundliche Technologien hilfreiche Instrumente für einen besseren Schutz und auch für eine effizientere Nutzung von Daten sein. Der EDSB schlägt zwei mögliche Vorgehensweisen vor, die einander nicht ausschließen:

— Schaffung eines Zertifizierungssystems für den Schutz der Privatsphäre und den Datenschutz ([25]) als Option für Hersteller und Nutzer von Informationssystemen, gegebenenfalls flankiert durch EU-Finanzmittel oder EU-Rechtsvorschriften.

([24]) Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgruppe nach Artikel 29), an der der EDSB mitwirkt, hat entschieden, intensiv an ihrem Beitrag zu dieser offenen Konsultation zu arbeiten.

([25]) Beispielhaft ist hier das Europäische Datenschutzgütesiegel (EuroPriSe) anzuführen.

— Einführung einer rechtlichen Verpflichtung für Hersteller und Nutzer von Informationssystemen, nur solche Systeme zu verwenden, die mit dem Grundsatz des „eingebauten Datenschutzes“ vereinbar sind.Hierdurch könnte eine Ausweitung des aktuellen Geltungsbereichs der Datenschutzgesetze erforderlich werden, um Hersteller für die von ihnen entwickelten Informationssysteme in die Verantwortung nehmen zu können ([26]).

Der EDSB schlägt vor, die beiden möglichen Vorgehensweisen in das Stockholmer Programm aufzunehmen.

V.4 **Externe Aspekte**

45. Ein weiteres Thema, auf das in der Mitteilung eingegangen wird, ist die Entwicklung und Förderung internationaler Standards für den Datenschutz. Derzeit gibt es zahlreiche Projekte zur Schaffung geeigneter global anwendbarer Standards, so beispielsweise seitens der Internationalen Konferenz der Datenschutzbeauftragten. In naher Zukunft könnten diese Bemühungen zu einem internationalen Übereinkommen führen. Der EDSB schlägt vor, diese Maßnahmen im Rahmen des Stockholmer Programms zu unterstützen.

46. In der Mitteilung kommt auch der Abschluss bilateraler Abkommen auf der Grundlage der gemeinsam mit den Vereinigten Staaten erzielten Fortschritte zur Sprache. Der EDSB teilt die Auffassung, dass ein klarer rechtlicher Rahmen für die Weitergabe von Daten an Drittstaaten geschaffen werden muss, und begrüßte deshalb die gemeinsam von EU und Vereinigten Staaten in der hochrangigen Kontaktgruppe geführten Beratungen über eine etwaige transatlantische Übereinkunft zum Datenschutz; gleichzeitig forderte er jedoch in bestimmten Fragen mehr Klarheit und Wachsamkeit ([27]). Vor diesem Hintergrund sind auch die in dem Bericht zur Innenpolitik enthaltenen Überlegungen zu einem euro-atlantischen Raum der Zusammenarbeit im Bereich der Freiheit, der Sicherheit und des Rechts mit Interesse zu betrachten, über den die Europäische Union dem Bericht zufolge bis 2014 eine Entscheidung treffen soll. Ein solcher Raum wäre ohne angemessene Datenschutzgarantien nicht realisierbar.

47. Der EDSB ist der Auffassung, dass die europäischen Datenschutzstandards, denen das Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ([28]) sowie die ständige Rechtsprechung des Europäischen Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte zugrundeliegen, das Schutzniveau in einem allgemeinen Übereinkommen mit den Vereinigten Staaten über Datenschutz und Datenaustausch vorgeben sollten. Ein solches allgemeines Übereinkommen könnte der Ausgangspunkt für Sondervereinbarungen über den Austausch personenbezogener Daten sein. Dies ist umso wichtiger, als es in Abschnitt 4.2.1 der Mitteilung heißt, dass die Europäische Union bei Bedarf Übereinkommen über die polizeiliche Zusammenarbeit schließen müsse.

48. Der EDSP ist sich der Notwendigkeit einer verbesserten internationalen Zusammenarbeit, in die in einigen Fällen auch Länder einbezogen werden müssen, die die Grundrechte nicht schützen, voll bewusst. Hierbei muss jedoch unbedingt berücksichtigt werden, dass eine solche internationale Zusammenarbeit zu einem großen Anstieg der erhobenen und international übermittelten Daten führen dürfte ([29]). Es ist daher unerlässlich, dass die Grundsätze einer rechtmäßigen Verarbeitung nach Treu und Glauben — sowie im Allgemeinen die Grundsätze eines fairen Verfahrens (due process) — auch für die Erhebung und die Übermittlung personenbezogener Daten über die Grenzen der Union hinweg gelten und dass personenbezogene Daten nur dann an Drittstaaten oder internationale Einrichtungen weitergegeben werden, wenn von den betreffenden dritten Parteien ein angemessener Schutz oder angemessene Garantien gewährleistet werden.

49. Abschließend empfiehlt der EDSB, im Stockholmer Programm herauszustellen, wie wichtig allgemeine Übereinkünfte mit den Vereinigten Staaten und anderen Drittstaaten über den Schutz und den Austausch von Daten sind, denen das innerhalb der Europäischen Union garantierte Schutzniveau zugrunde liegt. In einer allgemeineren Perspektive weist der EDSB darauf hin, wie wichtig es ist, in den Beziehungen zu Drittstaaten und internationalen Organisationen aktiv für die Achtung der Grundrechte, und insbesondere die Achtung des Datenschutzes einzutreten ([30]). Außerdem könnte im Stockholmer Programm ganz allgemein vorgesehen werden, dass für einen Austausch personenbezogener Daten mit Drittstaaten in diesen Drittstaaten ein angemessener Schutz oder sonstige angemessene Garantien gewährleistet sein müssen.

VI. **NUTZUNG VON INFORMATIONEN**

VI.1 **Einführung eines europäischen Informationsmodells**

50. Für die Europäische Union ist ein besserer Informationsaustausch ein grundlegendes politisches Ziel für den Raum der Freiheit, der Sicherheit und des Rechts. In Abschnitt 4.1.2 der Mitteilung wird hervorgehoben, dass es für die Sicherheit der Europäischen Union leistungsfähiger Systeme für den Informationsaustausch zwischen den nationalen Behörden und den europäischen Stellen bedarf. Der hohe Stellenwert des Informationsaustausches ist insofern erklärlich, als eine europäische Polizei, eine europäische Strafjustiz und eine europäische Grenzkontrollbehörde fehlen. Informationsbezogene Maßnahmen sind somit wesentliche Beiträge der Europäischen Union, die es den Behörden

([26]) Nutzer von Informationen fallen ebenso unter das Datenschutzgesetz wie die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter.

([27]) Vgl. die Stellungnahme des EDSB vom 11. November 2008 zu dem Abschlussbericht der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten, ABl. C 128 vom 6.6.2009, S. 1.

([28]) Übereinkommen Nr. 108 vom 28.1.1981.

([29]) Vgl. Schreiben des EDSB vom 28. November 2005 zu der Mitteilung der Kommission „Eine Strategie für die Außendimension des Raums der Freiheit, der Sicherheit und des Rechts“, abrufbar auf der Website des EDSB.

([30]) Durch die jüngste Rechtsprechung zu den Terroristen-Listen wird bestätigt, dass auch in den Beziehungen zu den Vereinten Nationen Garantien erforderlich sind, um sicherstellen zu können, dass Maßnahmen zur Bekämpfung des Terrorismus mit den EU-Grundrechtestandards vereinbar sind (Verbundene Rechtssachen C-402/05 P und C-415/05 P, Kadi and Al Barakaat Foundation gegen den Rat, Urteil vom 3. September 2008, noch nicht archiviert).

der Mitgliedstaaten ermöglichen, grenzüberschreitende Kriminalität wirksam zu bekämpfen und die Außengrenzen wirksam zu schützen. Dies trägt jedoch nicht nur zur Sicherheit der Bürger bei, sondern auch zu ihrer Freiheit — die Freizügigkeit wurde vorstehend bereits als einer der wichtigen Aspekte dieser Stellungnahme erwähnt — und zum Recht.

51. Genau aus diesen Gründen wurde der Grundsatz der Verfügbarkeit im Haager Programm eingeführt. Er beinhaltet, dass für die Bekämpfung von Kriminalität benötigte Informationen die Binnengrenzen der EU ohne Hindernisse überqueren sollten. Jüngste Erfahrungen verdeutlichen, dass es schwierig war, diesen Grundsatz in gesetzgeberische Maßnahmen umzusetzen. Der Vorschlag der Kommission für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit ([31]) vom 12. Oktober 2005 wurde vom Rat nicht akzeptiert. Die Mitgliedstaaten waren nicht bereit, die Konsequenzen des Grundsatzes der Verfügbarkeit uneingeschränkt zu tragen. Statt dessen wurden Rechtakte mit geringerer Tragweite ([32]) verabschiedet, wie beispielsweise der Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (Prümer Beschluss) ([33]).

52. Während der Grundsatz der Verfügbarkeit das Kernstück des Haager Programm war, scheint die Kommission nun einen weniger anspruchsvollen Ansatz zu verfolgen. Sie beabsichtigt, durch die Einführung des europäischen Informationsmodells den Informationsaustausch zwischen den Behörden der Mitgliedstaaten zu begünstigen. Der schwedische EU-Vorsitz vertritt eine ähnliche Auffassung ([34]). Er wird einen Vorschlag für eine Strategie für den Informationsaustausch vorlegen. Der Rat hat bereits die Beratungen über dieses anspruchsvolle Projekt einer EU-Strategie für das Informationsmanagement, das eng mit dem europäischen Informationsmodell verknüpft ist, aufgenommen. Der EDSB nimmt diese Entwicklungen mit großem Interesse zur Kenntnis und weist eindringlich darauf hin, dass bei diesen Projekten ein besonderes Augenmerk auf den Datenschutz gelegt werden sollte.

Das europäische Informationsmodell und der Datenschutz

53. Zunächst einmal sollte hervorgehoben werden, dass die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts nicht „technologiebestimmt" sein sollte, was so zu verstehen ist, dass die beinahe grenzenlosen Möglichkeiten, die die neuen Technologien bieten, immer an Hand relevanter Datenschutzgrundsätze überprüft und nur insoweit eingesetzt werden sollten, wie sie mit diesen Grundsätzen im Einklang stehen.

54. Der EDSB stellt fest, dass das Informationsmodell in der Mitteilung nicht ausschließlich als ein technisches Modell vorgestellt wird, sondern als ein Modell mit einer verstärkten strategischen Analysekapazität und gleichzeitig einer besseren Erfassung und Verarbeitung operativer Informationen. In der Mitteilung wird auch zugestanden, dass allgemeinpolitische Aspekte — wie Kriterien für die Erfassung, Weitergabe und Verarbeitung der Informationen — unter Beachtung der Datenschutzgrundsätze berücksichtigt werden müssen.

55. Informationstechnologie und rechtliche Bedingungen sind beide von grundlegender Bedeutung und werden dies auch weiterhin sein. Der EDSB begrüßt, dass in der Mitteilung von der Annahme ausgegangen wird, dass ein europäisches Informationsmodell nicht allein auf technischen Überlegungen basieren darf. Es ist von wesentlicher Bedeutung, dass Informationen lediglich bei Vorliegen eines konkreten Bedarfs aus Sicherheitsgründen und unter Berücksichtigung der Datenschutzgrundsätze erhoben, weitergegeben und verarbeitet werden dürfen. Der EDSB schließt sich auch uneingeschränkt der Auffassung an, dass ein Beobachtungsinstrument festgelegt werden muss, um feststellen zu können, wie der Informationsaustausch funktioniert. Er schlägt vor, dass der Rat diese Punkte im Stockholmer Programm näher festlegt.

56. Der EDSB betont in diesem Zusammenhang, dass Datenschutz mit dem Ziel, den Bürger zu schützen, nicht als etwas gesehen werden sollte, das einem effizienten Datenmanagement entgegensteht. Datenschutz liefert wichtige Werkzeuge dafür, die Speicherung von Informationen, den Zugang dazu und ihren Austausch zu verbessern. Zudem kann durch das Recht einer betroffenen Person, darüber Auskunft zu erhalten, welche sie betreffenden Informationen verarbeitet werden, und durch ihr Recht, fehlerhafte Angaben zu berichtigen, die Richtigkeit der in Datenverarbeitungssystemen enthaltenen Daten erhöht werden.

57. Datenschutzgesetze haben im Wesentlichen folgende Wirkung: Sind Daten für einen bestimmten rechtmäßigen Zweck erforderlich, so dürfen sie verwendet werden; sind die Daten nicht für einen präzise definierten Zweck erforderlich, so sollten personenbezogene Daten nicht verwendet werden. Im ersten Fall können durchaus ergänzende Maßnahmen erforderlich sein, um ausreichende Garantien zu bieten.

58. Der EDSB sieht jedoch kritisch, dass in der Mitteilung die „Bestimmung des künftigen Bedarfs" als Bestandteil des Informationsmodells betrachtet wird. Er betont, dass auch in Zukunft der Grundsatz der Zweckbindung der Leitgedanke beim Aufbau von Informationssystemen sein sollte ([35]). Dieser Grundsatz ist eine der wichtigsten Garantien, die das Datenschutzsystem dem Bürger zu geben vermag: der Bürger muss im Vorhinein wissen können, zu welchem Zweck ihn betreffende Daten erhoben werden, und er muss ebenso im Vorhinein wissen können, dass diese Daten insbesondere auch in Zukunft nur zu diesem Zweck verwendet werden. Diese Garantie ist auch in Artikel 8 der Charta der Grundrechte der Europäischen Union festgeschrieben. Zwar lässt der Grundsatz der Zweckbindung Ausnahmen zu, die insbesondere im Raum der Freiheit, der Sicherheit und des Rechts relevant sind, diese Ausnahmen sollten jedoch nicht für den Aufbau eines Systems bestimmend sein.

([31]) KOM(2005) 490 endg.

([32]) Im Hinblick auf die Verfügbarkeit enthält der Prümer Beschluss weitreichende Bestimmungen für die Nutzung biometrischer Daten (DNA und Fingerabdrücke).

([33]) ABl. L 210 vom 6.8.2008, S. 1.

([34]) Vgl. S. 23 des in Fußnote 5 erwähnten EU-Arbeitsprogramms der schwedischen Regierung.

([35]) Siehe Nummer 41.

Wahl der richtigen Systemarchitektur

59. Alles steht und fällt mit der Wahl der richtigen Systemarchitektur für den Informationsaustausch. Die Bedeutung einer geeigneten Informationssystemarchitektur wird in der Mitteilung anerkannt (Abschnitt 4.1.3), bedauerlicherweise jedoch nur in Bezug auf die Interoperabilität.

60. Der EDSB hebt einen weiteren Aspekt hervor: Im europäischen Informationsmodell sollten Datenschutzanforderungen Bestandteil der gesamten Systementwicklung sein und nicht nur als notwendige Voraussetzung für die Rechtmäßigkeit eines Systems betrachtet werden ([36]). Wie bereits unter Nummer 43 angesprochen, sollte auf das Konzept des „eingebauten Datenschutzes" zurückgegriffen werden, und es sollte der Notwendigkeit, die „besten verfügbaren Techniken" ([37]) zu ermitteln, Rechnung getragen werden. Das europäische Informationsmodell sollte auf beiden aufbauen. Konkret bedeutet dies, dass Informationssysteme, die zum Zwecke des Schutzes der öffentlichen Sicherheit konzipiert werden, immer nach dem Grundsatz des „eingebauten Datenschutzes" entwickelt werden sollten. Der EDSB empfiehlt dem Rat, diese Punkte in das Stockholmer Programm aufzunehmen.

Interoperabilität der Systeme

61. Der EDSB weist eindringlich darauf hin, dass Interoperabilität nicht nur eine rein technische Frage ist, sondern auch Auswirkungen auf den Schutz des Bürgers und insbesondere auf den Datenschutz hat. Unter dem Blickwinkel des Datenschutzes betrachtet, bietet die Interoperabilität von Systemen, wenn sie in geeigneter Weise hergestellt wird, deutliche Vorteile, da eine doppelte Datenspeicherung vermieden werden kann. Es liegt allerdings auch auf der Hand, dass dadurch, dass der Zugang zu Daten oder deren Austausch technisch ermöglicht wird, der tatsächliche Zugang zu diesen Daten bzw. ihr Austausch in vielen Fällen beträchtlich stimuliert wird. Mit anderen Worten, die Interoperabilität birgt das besondere Risiko der Zusammenschaltung von Datenbanken, die mit unterschiedlichen Zweckbestimmungen eingerichtet wurden ([38]). Hierdurch kann die strenge Zweckbindung von Datenbanken aufgeweicht werden.

62. Kurz gesagt, die einfache Tatsache, dass es technisch möglich ist, digitale Informationen zwischen interoperablen Datenbanken auszutauschen oder derartige Datenbanken zusammenzulegen, rechtfertigt kein Abweichen vom Grundsatz der Zweckbindung. Interoperabilität sollte in konkreten Einzelfällen auf eindeutigen und sorgfältig abgewogenen politischen Entscheidungen basieren. Der EDSB schlägt vor, dies im Stockholmer Programm konkret zu regeln.

VI.2 **Nutzung von zu anderen Zwecken erhobenen Informationen**

63. In der Mitteilung wird nicht ausdrücklich auf einen der wichtigsten Trends der letzten Jahre eingegangen, dass nämlich Daten, die von der Privatwirtschaft zu Geschäftszwecken erhoben wurden, zu Strafverfolgungszwecken verwendet werden. Dieser Trend beschränkt sich nicht nur auf Verkehrsdaten im Rahmen der elektronischen Kommunikation und die Fluggastdatensätze von Personen, die in (bestimmte) Drittländer fliegen ([39]), sondern ist auch schwerpunktmäßig im Finanzsektor feststellbar. Ein Beispiel dafür ist die Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung ([40]). Ein weiteres bekanntes und viel diskutiertes Beispiel betrifft die Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) ([41]); diese Daten benötigte das US-Finanzministerium für die Zwecke seines Programms zum Aufspüren der Finanzierungsquellen des Terrorismus.

64. Der EDSB ist der Auffassung, dass diesem Trend im Stockholmer Programm besondere Aufmerksamkeit gewidmet werden sollte. Dieser Trend kann als Abweichen vom Grundsatz der Zweckbindung betrachtet werden und bedeutet oftmals einen starken Eingriff in die Privatsphäre, da die Nutzung dieser Daten in großem Umfang Rückschlüsse auf das Verhalten des Einzelnen zulässt. Wenn immer derartige Maßnahmen vorgeschlagen werden, muss sehr eindeutig nachgewiesen werden können, dass eine derart in die Privatsphäre eingreifende Maßnahme erforderlich ist. Kann dieser Nachweis geführt werden, so muss sichergestellt werden, dass die Rechte des Einzelnen uneingeschränkt gewahrt werden.

65. Nach Auffassung des EDSB sollte die Nutzung von zu Geschäftszwecken erhobenen personenbezogenen Daten zu Strafverfolgungszwecken nur unter sehr strengen Bedingungen gestattet sein; so sollte beispielsweise Folgendes sichergestellt sein:

— Die Daten werden nur für einen ganz spezifischen Zweck genutzt, wie beispielsweise die Bekämpfung von Terrorismus oder Schwerkriminalität, wobei der Zweck von Fall zu Fall festzulegen ist.

— Die Datenübermittlung erfolgt vorzugsweise mittels eines „Push-Systems", nicht mittels eines „Pull-Systems" ([42]).

([36]) Vgl. die im Rahmen des Projektes PRISE entwickelten „Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies" (http://www.prise.oeaw.ac.at).

([37]) Unter der „besten verfügbaren Technik" ist der effizienteste und fortschrittlichste Entwicklungsstand von Tätigkeiten und entsprechenden Betriebsmethoden zu verstehen, der spezielle Techniken als praktisch geeignet erscheinen lässt, prinzipiell als Grundlage für informationstechnische und sicherheitstechnische Anwendungen und Systeme herangezogen zu werden, die mit den Anforderungen an den Schutz der Privatsphäre und den Datenschutz- und Sicherheitsanforderungen gemäß dem Regelungsrahmen der EU vereinbar sind.

([38]) Vgl. auch die Kommentare des EDSB vom 10. März 2006 zu der Mitteilung der Kommission über die Interoperabilität der europäischen Datenbanken, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Siehe z. B. Nummer 15.

([40]) ABl. L 309 vom 25.11.2005, S. 15.

([41]) Vgl. Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) der Datenschutzgruppe nach Artikel 29.

([42]) Bei einem „Push-System" sendet der für die Verarbeitung Verantwortliche die Daten auf Anfrage an die Strafverfolgungsbehörde. Bei einem „Pull-System" hat die Strafverfolgungsbehörde Zugriff auf die Datenbank des für die Verarbeitung Verantwortlichen und extrahiert Informationen aus dieser Datenbank. Bei einem „Pull-System" ist es für den für die Verarbeitung Verantwortlichen schwerer, seiner Verantwortung gerecht zu werden.

— Anfragen nach Daten sollten verhältnismäßig und sehr gezielt sein und prinzipiell auf Verdachtsmomenten gegen bestimmte Personen basieren.

— Routine-Suchläufe, Data Mining und Profiling sollten vermieden werden.

— Jede Nutzung der Daten zu Strafverfolgungszwecken sollte protokolliert werden, um eine wirksame Kontrolle der Nutzung durch die betroffene Person in Ausübung ihrer Rechte, durch die Datenschutzbehörden und durch die Justiz zu ermöglichen.

VI.3 **Informationssysteme und EU-Einrichtungen**

Informationssysteme mit oder ohne zentrale Speicherung ([43])

66. In den letzten Jahren ist die Zahl der sich auf EU-Rechtsvorschriften gründenden Informationssysteme im Bereich Freiheit, Sicherheit und Recht deutlich angestiegen. In einigen Fällen wurde ein System geschaffen, das eine zentrale Speicherung von Daten auf europäischer Ebene vorsieht, in anderen Fällen sehen die Rechtsvorschriften lediglich den Informationsaustausch zwischen einzelstaatlichen Datenbanken vor. Das Schengener Informationssystem ist wahrscheinlich das beste Beispiel für ein System mit zentraler Speicherung. Unter Datenschutzgesichtspunkten ist der Beschluss 2008/615/JI des Rates (Prümer Beschluss) ([44]) das bedeutendste Beispiel für ein System ohne zentrale Datenspeicherung, da hier ein umfangreicher Austausch biometrischer Daten zwischen den Behörden in den Mitgliedstaaten vorgesehen ist.

67. In der Mitteilung wird anschaulich dargelegt, dass der Trend zur Schaffung neuer Systeme sich fortsetzen wird. Ein erstes Beispiel dafür (siehe Abschnitt 4.2.2 der Mitteilung) ist ein Informationssystem, mit dem das Europäische Strafregisterinformationssystem (ECRIS) auf Staatsangehörige von Nicht-EU-Ländern ausgeweitet wird. Die Kommission hat bereits eine Studie über ein Europäisches Register für verurteilte Drittstaatsangehörige in Auftrag gegeben, das möglicherweise in eine zentrale Datenbank münden wird. Ein zweites Beispiel ist der ohne zentrale Speicherung erfolgende Informationsaustausch über in den Insolvenzregistern anderer Mitgliedstaaten registrierte natürliche Personen im Rahmen des elektronischen Rechtsverkehrs (Abschnitt 3.4.1 der Mitteilung).

68. Ein dezentrales System hätte unter dem Gesichtspunkt des Datenschutzes gewisse Vorteile. Die doppelte Speicherung von Daten, zum einen bei der Behörde des Mitgliedstaats und zum anderen im Zentralsystem, wird vermieden, die Zuständigkeit für die Daten ist eindeutig geregelt, da die Behörde des Mitgliedstaats die für die Verarbeitung verantwortliche Stelle ist, und die Kontrolle durch Justiz und Datenschutzbehörden kann auf der Ebene der Mitgliedstaaten erfolgen. Ein solches System hat aber auch Schwächen, wenn Daten mit Stellen ausgetauscht werden, für die eine andere Gerichtsbarkeit gilt, wenn beispielsweise gewährleistet sein muss, dass die Informationen sowohl im Herkunftsland als auch im Bestimmungsland auf dem neuesten Stand gehalten werden, und wenn es um die Frage geht, wie auf beiden Seiten für eine wirksame Kontrolle gesorgt werden kann. Noch schwieriger ist es, die Verantwortung für das technische System für den Austausch zuzuordnen. Diese Schwächen können dadurch vermieden werden, dass ein zentrales System geschaffen wird, in dem die Verantwortung zumindest für Teile des Systems (z. B. die technische Infrastruktur) bei den europäischen Einrichtungen liegt.

69. In diesem Zusammenhang wäre es hilfreich, grundlegende Kriterien auszuarbeiten, die für die Wahl eines zentralen oder eines dezentralen Systems sprechen, um so sicherzustellen, dass im konkreten Fall eine klare und umsichtige politische Wahl getroffen wird. Diese Kriterien können auf die Funktionsweise der Systeme selbst, aber auch auf den Schutz der über den Bürger gespeicherten Daten abstellen. Der EDSB schlägt vor, im Stockholmer Programm die Absicht zum Ausdruck zu bringen, entsprechende Kriterien auszuarbeiten.

Groß angelegte Informationssysteme

70. In Abschnitt 4.2.3.2 der Mitteilung wird kurz auf die Zukunft von groß angelegten Informationssystemen eingegangen, wobei ein Schwerpunkt auf das Schengener Informationssystem (SIS) und das Visa-Informationssystem (VIS) gelegt wird.

71. Dort wird neben Programmen für registrierte Reisende auch die Schaffung eines elektronischen Registriersystems für Ein- und Ausreisen in die bzw. aus den Hoheitsgebieten der Mitgliedstaaten erwähnt. Dieses System war von der Kommission zu einem früheren Zeitpunkt als Bestandteil des „Grenzpakets“ angekündigt worden und geht auf eine Initiative von Vizepräsident Frattini zurück ([45]). In einer vorläufigen Stellungnahme ([46]) hat sich der EDSB ziemlich kritisch zu diesem Vorschlag geäußert, da die Notwendigkeit für ein System, mit dem dergestalt in die Privatsphäre eingedrungen würde und das noch zusätzlich zu den bereits bestehenden Großsystemen eingerichtet würde, nicht hinreichend nachgewiesen war. Da dem EDSB keine weiteren Belege für die Notwendigkeit eines solchen Systems vorliegen, schlägt er dem Rat vor, den Vorschlag nicht in das Stockholmer Programm aufzunehmen.

72. In diesem Zusammenhang verweist der EDSB auf seine Stellungnahmen zu verschiedenen Initiativen auf dem Gebiet des Informationsaustauschs in der EU ([47]), in denen er zahlreiche Vorschläge und Bemerkungen zu den mit der Nutzung großer Datenbanken auf EU-Ebene verbundenen Datenschutzaspekten vorgelegt hat. Neben anderen Fragen hat der EDSB ein besonderes Augenmerk auf folgende

([43]) Unter zentraler Speicherung ist hier eine Speicherung auf zentraler europäischer Ebene zu verstehen, wohingegen dezentrale Speicherung als Speicherung auf der Ebene der Mitgliedstaaten zu verstehen ist.

([44]) Siehe Fußnote 33.

([45]) Mitteilung der Kommission mit dem Titel „Vorbereitung der nächsten Schritte für die Grenzverwaltung in der Europäischen Union“ vom 13.2.2008, KOM(2008) 69.

([46]) Vorläufige Stellungnahme des EDSB zu drei Mitteilungen der Kommission zum Grenzmanagement (KOM(2008) 69, KOM(2008) 68 und KOM(2008) 67) vom 3. März 2008, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) Im Einzelnen: Stellungnahme vom 23. März 2005 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt, ABl. C 181 vom 23.7.2005, S. 13, sowie Stellungnahme vom 19. Oktober 2005 zu drei Vorschlägen zum Schengener Informationssystem der zweiten Generation (SIS II), ABl. C 91 vom 19.4.2006, S. 38.

Punkte gelegt: die Notwendigkeit des Vorhandenseins strikter und bedarfsgerechter Garantien, die Verhältnismäßigkeit und die Notwendigkeit von Folgenabschätzungen, bevor in diesem Bereich überhaupt Maßnahmen vorgeschlagen oder getroffen werden. Er ist immer für ein angemessenes und datenschutzkonformes Gleichgewicht zwischen Sicherheitsanforderungen und dem Schutz der Privatsphäre der von den Systemen erfassten Einzelpersonen eingetreten. Den gleichen Standpunkt hat er auch bei der Aufsicht über die zentralen Teile der Systeme vertreten.

73. Der EDSB nutzt überdies die Gelegenheit, um eindringlich auf die Notwendigkeit eines kohärenten Ansatzes für den Informationsaustausch in der EU insgesamt hinzuweisen, den es im Hinblick auf die rechtliche, technische und aufsichtsbezogene Kohärenz zwischen den bereits bestehenden und den in der Entwicklung befindlichen Systemen zu verfolgen gilt. In der Tat ist heute — mehr als zuvor — eindeutig eine mutige und umfassende Zukunftsprojektion zu der Frage erforderlich, wie der Informationsaustausch in der EU und die Zukunft der groß angelegten Informationssysteme aussehen sollen. Nur gestützt auf eine solche Zukunftsprojektion kann ein elektronisches Registriersystem für Ein- und Ausreise in die bzw. aus den Hoheitsgebieten der Mitgliedstaaten überhaupt wieder ins Auge gefasst werden.

74. Der EDSB schlägt vor, im Stockholmer Programm die Absicht zu erklären, eine entsprechende Zukunftsprojektion zu entwickeln, die auch Überlegungen zum möglichen Inkrafttreten des Vertrags von Lissabon und dessen Auswirkungen auf Systeme, deren Rechtsgrundlage in der ersten und der dritten Säule begründet liegt, beinhalten sollte.

75. Schließlich wird in der Mitteilung noch die Errichtung einer neuen Agentur erwähnt, die gemäß der Mitteilung auch für das elektronische Registriersystem für die Ein- und Ausreise zuständig sein soll. Die Kommission hat in der Zwischenzeit einen Vorschlag für die Errichtung einer solchen Agentur vorgelegt ([48]). Der EDSB unterstützt diesen Vorschlag im Prinzip, da er bewirken kann, dass diese Systeme und auch der Datenschutz effizienter funktionieren. Er wird zu gegebener Zeit eine Stellungnahme zu diesem Vorschlag abgeben.

Europol und Eurojust

76. In der Mitteilung wird mehrfach auf die Rolle von Europol hingewiesen, und im Kapitel „Künftige Handlungsschwerpunkte" wird hervorgehoben, dass Europol in den Bereichen Koordinierung, Informationsaustausch und Aus- und Fortbildung eine zentrale Rolle übernehmen muss. Ebenso wird in Abschnitt 4.2.2 der Mitteilung auf die jüngsten Änderungen am Rechtsrahmen für die Zusammenarbeit zwischen Eurojust und Europol Bezug genommen und festgestellt, dass Eurojust weitere Befugnisse erhalten müsse, insbesondere bei Untersuchungen im Bereich des grenzüberschreitenden organisierten Verbrechens. Der EDSB schließt sich diesen Zielen uneingeschränkt an, sofern für geeignete Datenschutzgarantien gesorgt wird.

77. In diesem Zusammenhang begrüßt der EDSB den neuen Entwurf einer Vereinbarung zwischen Europol und Eurojust ([49]), die darauf abzielt, die Zusammenarbeit zwischen den beiden Einrichtungen zu verbessern und zu vertiefen und für einen effizienten Informationsaustausch zwischen beiden zu sorgen. Hierbei kommt einem effizienten und effektiven Datenschutz eine wichtige Rolle zu.

VI.4 **Nutzung biometrischer Daten**

78. Der EDSB stellt fest, dass in der Mitteilung nicht darauf eingegangen wird, dass in verschiedenen Rechtsinstrumenten der Europäischen Union zum Informationsaustausch, einschließlich der Rechtsakte zur Einrichtung der groß angelegten Informationssysteme, vermehrt die Nutzung biometrischer Daten vorgesehen ist. Dies ist bedauerlich, da es sich vom Standpunkt des Datenschutzes und des Schutzes der Privatsphäre aus hierbei um eine besonders wichtige und heikle Frage handelt.

79. Der EDSB erkennt zwar die allgemeinen Vorteile an, die die Nutzung biometrischer Daten bietet, er hat jedoch stets deutlich darauf hingewiesen, welche wesentlichen Auswirkungen die Nutzung dieser Daten auf die Rechte des Einzelnen hat, und hat stets die Einführung strenger Garantien für die Nutzung biometrischer Daten für jedes einzelne System vorgeschlagen. Das jüngste Urteil des Europäischen Gerichtshofs für Menschenrechte in der Rechtssache S. und Marper gegen das Vereinigte Königreich ([50]) enthält nützliche Hinweise in diesem Zusammenhang, insbesondere was die Rechtfertigung und die Grenzen der Nutzung biometrischer Daten betrifft. Durch die Verwendung insbesondere von DNA-Informationen können sensible Informationen über Einzelpersonen bekannt werden, auch da die technischen Möglichkeiten, um aus der DNA Informationen zu gewinnen, noch zunehmen. Werden biometrische Daten in großem Umfang in Informationssystemen verwendet, besteht außerdem ein Problem wegen der Ungenauigkeiten, die zwangsläufig mit der Erhebung und dem Abgleich biometrischer Daten verbunden sind. Daher sollte der EU-Gesetzgeber bei der Nutzung dieser Daten zurückhaltend sein.

80. Eine weitere, in den letzten Jahren immer wieder aufgeworfene Frage betrifft die Verwendung von Fingerabdrücken von Kindern und älteren Menschen angesichts der Tatsache, dass biometrische Systeme im Hinblick auf diese Altersgruppen inhärente Mängel aufweisen. Der EDSB hat eine eingehende Studie gefordert, um die Genauigkeit der Systeme angemessen zu ermitteln ([51]). Er hat eine Altersgrenze von 14 Jahren vorgeschlagen, es sei denn, die Studie erbrächte anderweitige Ergebnisse. Der EDSB schlägt vor, diese Frage im Stockholmer Programm zu thematisieren.

([48]) Vorschlag der Kommission vom 24. Juni 2009 für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung einer Agentur für das Betriebsmanagement des Schengener Informationssystems (SIS II), des Visa-Informationssystems (VIS), von EURODAC und von anderen IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (Dokument KOM(2009) 293/2 endgültig).

([49]) Der vom Rat gebilligte Entwurf einer Vereinbarung muss noch von beiden Parteien unterzeichnet werden. Siehe Öffentliches Register des Rates:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/de/09/st10/st10107.de09.pdf

([50]) Gemeinsame Beschwerden 30562/04 und 30566/04, S. und Marper gegen das Vereinigte Königreich, Urteil vom 4. Dezember 2008, EGMR, noch nicht archiviert.

([51]) Stellungnahme vom 26. März 2008 zu dem Vorschlag für eine Verordnung zur Änderung der Verordnung (EG) Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. C 200 vom 6.8.2008, S. 1.

81. Vor diesem Hintergrund wäre es nach Auffassung des EDSB nützlich, grundlegende Kriterien für die Verwendung biometrischer Daten festzulegen. Damit sollte sichergestellt werden, dass diese Daten nur dann verwendet werden, wenn es erforderlich, angemessen und verhältnismäßig ist und der Gesetzgeber einen bestimmten, genau festgelegten und rechtmäßigen Zweck geltend machen kann. Präziser formuliert bedeutet dies, dass biometrische Daten und insbesondere DNA-Daten nicht verwendet werden sollten, wenn durch den Rückgriff auf andere, weniger sensible Informationen die gleiche Wirkung erzielt werden kann.

VII. **ZUGANG DER BÜRGER ZUR JUSTIZ UND ELEKTRONISCHER RECHTSVERKEHR**

82. Technische Instrumente werden auch genutzt werden, um die justizielle Zusammenarbeit zu verbessern. In Abschnitt 3.4.1 der Mitteilung wird der elektronische Rechtsverkehr (E-Justiz) als ein Mittel vorgestellt, das den Zugang der Bürger zur Justiz vereinfacht. Der elektronische Rechtsverkehr wird über ein Portal abgewickelt, das Informationen und Videokonferenzen als Bestandteil des rechtlichen Verfahrens bietet. Außerdem eröffnet er die Möglichkeit von Online-Verfahren, geplant ist darüber hinaus die Vernetzung nationaler Register wie beispielsweise der Insolvenzregister. Der EDSB stellt fest, dass in der Mitteilung keine neuen Initiativen zum elektronischen Rechtsverkehr erwähnt werden, sondern dass darin lediglich die Konsolidierung bereits eingeleiteter Maßnahmen vorgesehen ist. Der EDSB ist im Anschluss an die Stellungnahme, die er am 19. Dezember 2008 zu der Mitteilung der Kommission mit dem Titel „Eine europäische Strategie für die e-Justiz“ abgegeben hat ([52]), in einige dieser Maßnahmen eingebunden.

83. Bei dem elektronischen Rechtsverkehr handelt es sich um ein Projekt mit hochgesteckten Zielen, das volle Unterstützung benötigt. Es kann tatsächlich Verbesserungen des Justizsystems in Europa und des Rechtsschutzes des Bürgers bewirken. Es ist ein großer Schritt auf dem Weg zu einem europäischen Rechtsraum. Vor dem Hintergrund dieser positiven Bewertung sind dennoch einige Anmerkungen zu machen:

— Die für den elektronischen Rechtsverkehr genutzten technischen Systeme sollten nach dem Grundsatz des „eingebauten Datenschutzes“ entwickelt werden. Wie bereits weiter oben im Zusammenhang mit dem europäischen Informationsmodell festgestellt, steht und fällt alles mit der Wahl der richtigen Systemarchitektur.

— Vernetzung und Interoperabilität der Systeme sollten dem Grundsatz der Zweckbindung genügen.

— Zuständigkeiten und Verantwortung der verschiedenen Akteure sollten eindeutig festgelegt sein.

— Es sollte im Vorhinein analysiert werden, wie sich die Vernetzung nationaler Register, die heikle personenbezogene Daten enthalten, wie beispielsweise die Insolvenzregister, auf den Einzelnen auswirken.

VIII. **SCHLUSSFOLGERUNGEN**

84. Der EDSB hält es für richtig, dass in der Mitteilung dem Schutz der Grundrechte und insbesondere dem Schutz personenbezogener Daten als einer der zentralen Fragen für die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts besondere Bedeutung beigemessen wurde. Der EDSB ist der Auffassung, dass in der Mitteilung zu Recht für ein Gleichgewicht zwischen dem Bedarf an geeigneten Instrumenten zur Wahrung der Sicherheit der Bürger und dem Schutz ihrer Grundrechte eingetreten wird. In der Mitteilung wird eingeräumt, dass dem Schutz personenbezogener Daten mehr Bedeutung beigemessen werden sollte.

85. Der EDSB stimmt dem Abschnitt 2.3 der Mitteilung, in dem unabhängig vom Inkrafttreten des Vertrags von Lissabon eine umfassende, alle Zuständigkeitsbereiche der Europäischen Union abdeckende Datenschutzregelung gefordert wird, uneingeschränkt zu. In diesem Zusammenhang empfiehlt er,

— die Notwendigkeit einer klaren und langfristigen Zukunftsprojektion für eine solche umfassende Regelung in das Stockholmer Programm aufzunehmen,

— die in diesem Bereich erlassenen Maßnahmen, ihre konkrete Umsetzung und ihre Wirksamkeit zu bewerten und dabei die negativen Auswirkungen auf die Privatsphäre und die Wirksamkeit der Maßnahmen für die Strafverfolgung zu berücksichtigen,

— die Notwendigkeit eines neuen rechtlichen Rahmens, der unter anderem an die Stelle des Rahmenbeschlusses 2008/977/JI des Rates treten soll, als einen Handlungsschwerpunkt in das Stockholmer Programm aufzunehmen.

86. Der EDSB begrüßt die Absicht der Kommission die Datenschutzgrundsätze zu bekräftigen, die mit der von der Kommission bei der Konferenz „Personenbezogene Daten — größere Nutzung, größerer Schutz“ vom 19. und 20. Mai 2009 angekündigten offenen Konsultation in einen Zusammenhang gestellt werden müssen. Zum Inhalt hebt der EDSB hervor, welche Bedeutung dem Grundsatz der Zweckbindung als einem der Eckpfeiler der Datenschutzvorschriften zukommt und wie wichtig es ist, sich auf die Möglichkeiten zur wirksameren Anwendung der Datenschutzgrundsätze zu konzentrieren, indem Instrumente genutzt werden, die die Befugnisse der für die Verarbeitung der Daten Verantwortlichen stärken.

87. Der „eingebaute Datenschutz“ und datenschutzfreundliche Technologien könnten durch folgende Maßnahmen vorangebracht werden:

— Schaffung eines Zertifizierungssystems für den Schutz der Privatsphäre und den Datenschutz als Option für Hersteller und Nutzer von Informationssystemen;

— Einführung einer rechtlichen Verpflichtung für Hersteller und Nutzer von Informationssystemen, nur solche Systeme zu verwenden, die mit dem Grundsatz des „eingebauten Datenschutzes“ vereinbar sind.

88. Bezüglich der externen Aspekte des Datenschutz spricht der EDSB folgende Empfehlungen aus:

— Im Stockholmer Programm sollte hervorgehoben werden, wie wichtig allgemeine Übereinkünfte über den Datenschutz und den Datenaustausch mit den Vereinigten Staaten und anderen Drittstaaten sind.

([52]) Stellungnahme des EDSB vom 19. Dezember 2008 zu der Mitteilung der Kommission „Eine europäische Strategie für die e-Justiz,“ ABl. C 128 vom 6.6.2009, S. 13.

— In den Beziehungen zu Drittstaaten und zu internationalen Organisationen sollte aktiv für die Achtung der Grundrechte und insbesondere des Datenschutzes eingetreten werden.

— Im Stockholmer Programm sollte vorgesehen werden, dass für einen Austausch personenbezogener Daten mit Drittstaaten in diesen Drittstaaten ein angemessener Schutz oder angemessene Garantien gewährleistet werden müssen.

89. Der EDSB nimmt die Entwicklungen zur Einführung einer Strategie der Europäischen Union für das Informationsmanagement und eines europäischen Informationsmodells mit großem Interesse zur Kenntnis und weist eindringlich darauf hin, dass bei diesen Projekten ein besonderes Augenmerk auf Datenschutzaspekte gelegt werden sollte, was im Stockholmer Programm weiter auszuführen wäre. Die Systemarchitektur für den Informationsaustausch sollte auf den Grundsätzen des „eingebauten Datenschutzes“ und den „besten verfügbaren Techniken“ aufbauen.

90. Die einfache Tatsache, dass es technisch möglich ist, digitale Informationen zwischen interoperablen Datenbanken auszutauschen oder derartige Datenbanken zusammenzulegen, rechtfertigt kein Abweichen vom Grundsatz der Zweckbindung. Interoperabilität sollte in konkreten Einzelfällen auf eindeutigen und sorgfältig abgewogenen politischen Entscheidungen basieren. Der EDSB schlägt vor, dies im Stockholmer Programm konkret zu regeln.

91. Die Nutzung von zu Geschäftszwecken erhobenen personenbezogenen Daten zu Strafverfolgungszwecken sollte nach Auffassung des EDSB nur unter sehr strengen Bedingungen gestattet sein, die in Nummer 65 der vorliegenden Stellungnahme näher ausgeführt sind.

92. Weitere Vorschläge zur Nutzung personenbezogener Informationen:

— Es sollten grundlegende Kriterien für die Wahl zwischen zentralen und dezentralen Systemen ausgearbeitet werden, und das Stockholmer Programm sollte einen Hinweis darauf enthalten, dass beabsichtigt wird, derartige Kriterien zu erarbeiten.

— Das Vorhaben, neben Programmen für registrierte Reisende ein elektronisches Registriersystem für die Ein- und Ausreise in die bzw. aus den Hoheitsgebieten der Mitgliedstaaten einzurichten, sollte keinen Eingang in das Stockholmer Programm finden.

— Die Ausweitung der Kompetenzen von Europol und Eurojust sollte ebenso unterstützt werden wie die jüngst zwischen Europol und Eurojust erarbeitete neue Vereinbarung.

— Es sollten grundlegende Kriterien für die Nutzung biometrischer Daten erarbeitet werden, durch die sichergestellt wird, dass diese Daten nur dann verwendet werden, wenn es erforderlich, angemessen und verhältnismäßig ist und der Gesetzgeber einen bestimmten, genau festgelegten und rechtmäßigen Zweck geltend machen kann. DNA-Daten sollte nicht verwendet werden, wenn durch den Rückgriff auf andere, weniger sensible Informationen die gleiche Wirkung erzielt werden kann.

93. Der EDSB befürwortet den elektronischen Rechtsverkehr und hat angemerkt, wie dieses Projekt verbessert werden könnte (vgl. Nummer 83).

Geschehen zu Brüssel am 10. Juli 2009.

Peter HUSTINX

Europäischer Datenschutzbeauftragter