Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch“

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE -

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

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

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

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 28 Absatz 2,[2]

gestützt auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008[3] über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden -

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1.1. Konsultation des EDSB

1. Am 7. Dezember 2012 nahm die Kommission eine Mitteilung mit dem Titel „Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch“ („Mitteilung“) an.[4] Am selben Tag nahm die Kommission einen Bericht zur Durchführung des Beschlusses 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] ABl. L 350 vom 30.12.2008, S. 60.
[4] COM(2012)735 final.

Terrorismus und der grenzüberschreitenden Kriminalität („Prümer Beschluss“) an.[5] Auf diesen Bericht wird in der vorliegenden Stellungnahme nicht eigens eingegangen; er wird an dieser Stelle lediglich zum besseren Verständnis des Kontexts erwähnt.

2. Vor der Annahme der Mitteilung erhielt der EDSB Gelegenheit, informell Kommentare abzugeben. Er begrüßt, dass einige seiner Kommentare in die Mitteilung eingeflossen sind.

1.2. Hintergrund und Ziele der Mitteilung

3. Das Stockholmer Programm[6] verfolgt das Ziel, künftige Herausforderungen zu bewältigen und den Raum der Freiheit, der Sicherheit und des Rechts mit Maßnahmen weiter zu stärken, in deren Mittelpunkt die Interessen und Bedürfnisse der Bürger stehen. Dort sind die Prioritäten der EU im Bereich Justiz und Inneres für den Zeitraum 2010-2014 und strategische Leitlinien für die legislative und operative Planung im Bereich Freiheit, Sicherheit und Recht im Einklang mit Artikel 68 des Vertrags über die Arbeitsweise der Europäischen Union („AEUV“) festgelegt[7].

4. Das Stockholmer Programm erkennt insbesondere das Erfordernis der Kohärenz und Konsolidierung bei der Entwicklung von Informationsmanagement und Informationsaustausch im Bereich der inneren Sicherheit in der EU an und ersucht den Rat und die Kommission, die Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU umzusetzen, was ein solides Datenschutzregime einschließt. In diesem Zusammenhang fordert das Stockholmer Programm die Kommission ebenfalls auf, zu prüfen, ob die Entwicklung eines europäischen Informationsaustauschmodells auf der Grundlage einer Sichtung des bestehenden Instrumentariums im Bereich des Informationsaustauschs in der EU erforderlich ist. Bei dieser Sichtung soll festgestellt werden, ob diese Instrumente wie ursprünglich vorgesehen funktionieren und den Zielvorgaben der Strategie für das Informationsmanagement entsprechen[8].

5. Im Nachgang zum Stockholmer Programm veröffentlichte die Kommission im Juli 2010 eine Mitteilung[9] („Mitteilung von 2010“), die einen vollständigen Überblick über die schon bestehenden, noch in der Umsetzung begriffenen oder in Betracht gezogenen Maßnahmen auf EU-Ebene bietet, mit denen die Erhebung, die Speicherung und der grenzüberschreitende Austausch personenbezogener Daten zu Zwecken der Strafverfolgung und Migrationssteuerung geregelt wird.

---

[5] COM(2012)732 final

[6] Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, Ratsdokument 5731/10, 3.3.2010.

[7] Vertrag über die Arbeitsweise der Europäischen Union, ABl. C 83 vom 30.3.2010, S. 47.

[8] Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, Ratsdokument 5731/10, Abschnitt 4.2.2.

[9] Mitteilung der Kommission vom 20. Juli 2010 an das Europäische Parlament und den Rat „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“, KOM(2010) 385 endgültig.

6. Die hier zu prüfende Mitteilung ist eine Antwort auf das Stockholmer Programm und baut auf der Mitteilung von 2010 auf; sie stellt eine Bestandsaufnahme des grenzüberschreitenden Informationsaustauschs in der EU in der Praxis dar und formuliert Empfehlungen für mögliche Verbesserungen.

2. KOMMENTARE

2.1. Allgemeine Kommentare

Bedarf an besserem Informationsaustausch unter Wahrung der Grundrechte

7. Wie bereits in früheren Stellungnahmen[10], erkennt der EDSB an, dass ein besserer Informationsaustausch ein politisches Kernziel für die Europäische Union im Bereich Freiheit, Sicherheit und Recht darstellt. Diese Betonung des Informationsaustauschs ist in Ermangelung einer europäischen Polizei, eines europäischen Strafjustizsystems und völlig harmonisierter europäischer Grenzkontrollen nur allzu logisch. Maßnahmen im Bereich Information leisten daher einen wesentlichen Beitrag der Europäischen Union, damit die nationalen Behörden der Mitgliedstaaten wirksam gegen grenzübergreifende Kriminalität vorgehen und die Außengrenzen wirksam schützen können.

8. Mit diesen Maßnahmen sollte allerdings nicht nur die Sicherheit der Bürger gewährleistet werden; sie sollten in unserer europäischen Gesellschaft auch in vollem Einklang mit den Grundrechten, einschließlich des Rechts auf Schutz personenbezogener Daten, stehen. Dies ist umso wichtiger, als der Austausch von Informationen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in großem Umfang personenbezogene Daten umfasst. Die Verarbeitung personenbezogener Daten in diesem Bereich birgt besondere Risiken für die betroffenen Personen und erfordert daher ein hohes Maß an Datenschutz.

9. Der EDSB begrüßt, dass dem Datenschutz in der Mitteilung generell Aufmerksamkeit geschenkt wurde. Er begrüßt, dass in der Mitteilung auf folgende Kerngrundsätze verwiesen wird: i) Garantien für Grundrechte, insbesondere das Recht auf den Schutz der Privatsphäre und auf den Schutz personenbezogener Daten, und ii) das Erfordernis der Notwendigkeit, das bedeutet, dass eine Einschränkung des Rechts auf den Schutz der Privatsphäre nur gerechtfertigt sein kann, wenn sie rechtmäßig ist, ein rechtmäßiges Ziel verfolgt und in einer demokratischen Gesellschaft notwendig ist. In der Mitteilung wird ferner auf den wesentlichen Charakter von Überprüfungen der Notwendigkeit sowie der Zweckbindung hingewiesen.[11]

10. Der EDSB vermerkt ferner positiv, dass in der Mitteilung die Notwendigkeit betont wird, für hohe Datenqualität, Datensicherheit und Datenschutz zu sorgen, und dass sie Folgendes unterstreicht: „Unabhängig von der Kombination oder

[10] Siehe beispielsweise die Stellungnahme des EDSB vom 10. Juli 2009 zur Mitteilung der Kommission an das Europäische Parlament und den Rat über einen Bereich der Freiheit, der Sicherheit und des Rechts im Dienste des Bürgers, ABl. C 276 vom 17.11.2009, S. 8, und Stellungnahme des EDSB vom 7. Oktober 2009 über die Vorschläge betreffend den Zugang von Strafverfolgungsbehörden zu EURODAC, ABl. C 92 vom 10.4.2010, S. 1.

[11] Siehe Punkt 2.5 der Mitteilung.

Sequenz sind die für jedes Instrument geltenden Regeln zum Datenschutz, zur Datensicherheit und zur Datenqualität sowie die Bestimmungen zur Zweckbestimmung des Instruments einzuhalten".[12]

Kontext bereits verfügbarer Instrumente

11. Die Mitteilung besagt eingangs, dass der Informationsaustausch insgesamt gut funktioniert, und fährt dann fort, dass weder neue Strafverfolgungsdatenbanken noch neue Instrumente für den Informationsaustausch auf EU-Ebene erforderlich sind, dass aber vorhandene Instrumente besser angewandt werden sollten. Der EDSB begrüßt diese Schlussfolgerung. In Anbetracht der Tatsache, dass seine Vielzahl von Systemen für den grenzüberschreitenden Informationsaustausch Risiken für den Schutz personenbezogener Daten und ein Eindringen in die Privatsphäre mit sich bringt, hat sich der EDSB in verschiedenen Stellungnahmen dafür eingesetzt, vor der Schaffung eines neuen Instruments erst einmal gründlich und mit Blick auf die aktuelle Situation die Frage zu prüfen, ob eine vollständige Anwendung der bestehenden Instrumente nicht ausreichen würde.[13]

12. Im Mittelpunkt der Mitteilung steht der Einsatz folgender vier EU-Instrumente durch die Mitgliedstaaten: Schwedische Initiative[14], Prümer Beschlüsse[15], Europol[16] und Schengener Informationssystem[17]. Sie geht nicht auf alle bestehenden und geplanten EU-Instrumente für die polizeiliche und justizielle Zusammenarbeit in Strafsachen ein und erwähnt beispielsweise auch nicht das bereits bestehende Europäische Strafregisterinformationssystem für EU-Staatsangehörige.[18] Weiter werden in der Mitteilung zwar andere EU-Instrumente

[12] Siehe Punkt 2.3 der Mitteilung.

[13] Siehe beispielsweise die Stellungnahme des EDSB vom 5. September 2012 zum Zugang von Strafverfolgungsbehörden zu EURODAC, die Stellungnahme des EDSB 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", die Stellungnahme des EDSB vom 24. November 2010 zur Mitteilung der Kommission an das Europäische Parlament und den Rat „EU-Politik zur Terrorismusbekämpfung: wichtigste Errungenschaften und künftige Herausforderungen", die Stellungnahme des EDSB vom 20. Dezember 2007 zum Entwurf für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, und die Stellungnahme des EDSB vom 19. Oktober 2005 zu drei Vorschlägen betreffend das Schengener Informationssystem der zweiten Generation (SIS II).

[14] Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden, ABl. L 386 vom 29.12.2006, S. 89.

[15] Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. L 210 vom 6.8.2008, S. 1, und Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. L 210 vom 6.8.2008, S. 12.

[16] Beschluss 2009/371/JI des Rates zur Errichtung des Europäischen Polizeiamtes, ABl. L 121 vom 15.5.2009, S. 37.

[17] Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205 vom 7.8.2007, S. 63.

[18] Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, ABl. L 93 vom 7.4.2009, S. 23, und Beschluss 2009/316/JI des Rates vom 6. April 2009 zur Einrichtung des

(z. B. Zollinformationssystem, Visa-Informationssystem, EURODAC, EUROSUR) oder Initiativen (z. B. die Vorschläge für ein Einreise-/Ausreise-System) im Bereich Freiheit, Sicherheit und Recht erwähnt, doch werden sie nicht näher analysiert.

13. Schließlich weist der EDSB darauf hin, dass auch Rechtsinstrumente aus anderen Bereichen als Freiheit, Sicherheit und Recht berücksichtigt werden sollten, da sie zunehmend an Bedeutung gewinnen (siehe die unter Punkt 16 genannten Punkte).

Tendenzen bei Ermittlungsmethoden

14. Neue Technologien haben dazu geführt, dass immer mehr Informationen verfügbar sind und diese Informationen auf sehr verschiedene Weise verwendet werden. In einer Informationsgesellschaft besteht bei Strafverfolgungsbehörden logischerweise die Neigung, zunehmend die in offenen Quellen verfügbaren Informationen zu nutzen und sie unter Einsatz ausgefeilter IT-Tools miteinander zu verknüpfen. Technologische Erscheinungen wie Cloud Computing, soziale Netzwerke, Mauterhebung und Geräte zur Standortermittlung sowie die Verknüpfung und Weitergabe von Daten aus verschiedenen Datenbanken oder der Einsatz von Analysewerkzeugen zur Vorhersage menschlichen Verhaltens haben die Art und Weise der Erhebung und Weiterverarbeitung von Daten grundlegend verändert. Arbeitsmethoden von Strafverfolgungsbehörden wie Data Mining und Profiling werden immer pro-aktiver, und Ermittlungen erfolgen aufgrund allgemeiner Entwicklungen, mitunter ohne konkrete Verdachtsmomente, aber unter Einsatz leistungsstarker IT-Tools.

15. Generell besteht zunehmend die Tendenz, Strafverfolgungsbehörden Zugriff auf verfügbare Daten zu gewähren, die in Vergangenheit, Gegenwart oder Zukunft für Zwecke erhoben wurden bzw. werden, die anfänglich nichts mit der Bekämpfung der Kriminalität zu tun haben und Personen betreffen, die eigentlich keiner Straftat verdächtigt werden. Immer häufiger wird Strafverfolgungsbehörden umfassender Zugriff auf diverse Großinformations- und Identifizierungssysteme gewährt oder wird ein solcher Zugriff geplant, wie sie beispielsweise in den Bereichen Einwanderung oder Grenzkontrollen eingerichtet wurden[19].

Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI, ABl. L 93 vom 7.4.2009, S. 33.

[19] Siehe beispielsweise den Beschluss 2008/633/JHA des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008, S. 129; den geänderten Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) 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) und für der Strafverfolgung dienende Anträge der Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit EURODAC-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung), COM(2012) 254 final, 30. Mai 2012, und den Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union, COM(2013) 95 final, 28. Februar 2013.

16. In der Vergangenheit gab es eine klare Trennung zwischen der Tätigkeit der Strafverfolgungsbehörden und der des privaten Sektors: Strafverfolgungsaufgaben wurden von eigens dafür bestimmten Behörden wahrgenommen, und private Akteure wurden nur fallweise aufgefordert, diesen Behörden bei einem konkreten Verdacht Daten zu übermitteln. Heute besteht die Tendenz, von privaten Akteuren eine systematische Zusammenarbeit mit Strafverfolgungsbehörden zu verlangen. Betroffen von dieser Tendenz sind beispielsweise Verkehrsdaten aus der elektronischen Kommunikation[20] und die Passagierdaten natürlicher Personen, die in (bestimmte) Drittländer fliegen[21], sie verbreitet sich allerdings auch im Finanzsektor[22].

17. Die Verfügbarkeit immer größerer Datenmengen außerhalb des Bereichs der Strafverfolgung sowie der Einsatz neuer, leistungsstarker IT-Tools durch die Strafverfolgungsbehörden tragen in gewisser Weise dazu bei, dass derzeit eine Verlagerung stattfindet: Es werden weniger Personen überwacht, die im Verdacht stehen, eine Straftat begangen zu haben oder an ihr beteiligt gewesen zu sein, oder bei denen aufgrund der Faktenlage berechtigter Grund zu der Annahme besteht, dass sie Straftaten begehen werden; stattdessen findet eine eher allgemeine Überwachung statt, bei der *a priori* alle Personen als potenzielle Gesetzesbrecher gelten und daher zu überwachen sind.

Konsequenzen

18. Aufgrund dieser weit reichenden Entwicklungen ist es erforderlich, das Gleichgewicht zwischen Strafverfolgungszwecken und dem Schutz der Grundrechte von Menschen zu überdenken und möglicherweise neu zu bestimmen. Es sei beispielsweise darauf hingewiesen, dass sich bei einer Sammlung von Informationen durch Überwachungsmethoden außerhalb eines konkreten Kriminalfalls auch der Kontext des Schutzes der Grundrechte ändert. Man könnte nun argumentieren, dass ohne einen bei Gericht anhängigen Fall der Grundsatz des fairen Verfahrens (Artikel 6 der Europäischen Menschenrechtskonvention) nicht angewandt werden kann und dass daher Erwägungen des Datenschutzes und des Schutzes der Privatsphäre an Bedeutung gewinnen sollten.

---

[20] 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.

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

[22] 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 (ABl. L 309 vom 25.11.2005, S. 15) (wird derzeit überarbeitet). Siehe ferner die Mitteilung der Kommission an das Europäische Parlament und den Rat vom 13. Juli 2011 „Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung", KOM(2011) 429 endgültig.

19. Das bedeutet, dass an erster Stelle Überlegungen über die Wirksamkeit von Datenschutzgrundsätzen im Lichte des technologischen Wandels sowie über die zunehmende Erhebung und Verwendung von Daten für Strafverfolgungszwecke angestellt werden müssen. Daraus können sich Anpassungen und/oder weitere Garantien ergeben.

20. Zweitens besteht heute mehr denn je mit Blick auf IT-Großsysteme und die zunehmende Verwendung von Daten, die ursprünglich für andere Zwecke als die Verbrechensbekämpfung erhoben wurden, eindeutiger Bedarf an einem gründlichen Nachdenken über den Informationsaustausch in der EU. Dabei sollte auch darüber nachgedacht werden, ob der derzeit zu beobachtende Trend zu einer breit angelegten, systematischen und proaktiven Überwachung nicht verdächtiger Personen die öffentliche Sicherheit wirklich verbessert und ob er tatsächlich einen Beitrag zur Bekämpfung der Kriminalität leistet.

21. Der EDSB begrüßt die Mitteilung als einen ersten Schritt auf dem Weg zu einer umfassenden Evaluierung und fordert die Kommission auf, die oben erwähnten Überlegungen anzustellen, deren Ergebnis eine umfassende, integrierte und durchstrukturierte EU-Politik für das Management von Informationen und des Informationsaustauschs in diesem Bereich sein sollte.

Beziehung zum bestehenden und zum vorgeschlagenen Datenschutzrahmen

22. Der EDSB hält fest, dass ein kohärenter und umfassender Rechtsrahmen für den Datenschutz unbedingt gewährleistet sein muss. Ein erster wichtiger Schritt in diesem Zusammenhang war die Annahme des Rahmenbeschlusses 2008/977/JI des Rates[23]. Dieses Rechtsinstrument kann allerdings nicht als umfassender Rahmen bezeichnet werden, hauptsächlich, weil seine Bestimmungen nicht generell anwendbar sind. Sie gelten nicht in Fällen, in denen personenbezogene Daten aus dem Mitgliedstaat stammen, der sie verwendet[24]. Zweitens sollten die anderen für den Bereich Freiheit, Sicherheit und Recht geltenden Datenschutzinstrumente weiter harmonisiert und konsolidiert werden.

23. Der EDSB weist nachdrücklich darauf hin, dass die laufenden Diskussionen über den Vorschlag der Kommission vom 25. Januar 2012 für eine Richtlinie über die Verarbeitung personenbezogener Daten für Strafverfolgungszwecke[25] die Kommission nicht davon abhalten sollten, schon jetzt eine Bestandsaufnahme der Probleme und Risiken des Datenschutzes vorzunehmen und sich Gedanken über mögliche Verbesserungen im aktuellen rechtlichen Kontext zu machen. Ganz im Gegenteil: Die Diskussionen über den Richtlinienvorschlag könnten sich

[23] 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.

[24] Siehe auch die Stellungnahme des EDSB 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 endgültig), ABl. C 47 vom 25.2.2006, S. 27.

[25] Vorschlag vom 25. Januar 2012 für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, COM(2012) 10 final.

inspirierend auf die weitere Entwicklung des Europäischen Modells für den Informationsaustausch auswirken. Gute Beispiele in diesem Zusammenhang sind die Diskussionen über klare Unterscheidungen bei der Verarbeitung von Daten über verdächtige und nicht verdächtige Personen. Der EDSB empfiehlt, diese Konzepte im Zusammenhang mit dem Europäischen Modell für den Informationsaustausch näher zu analysieren.

24. Der EDSB hält fest, dass in der Mitteilung von dem Richtlinienvorschlag der Kommission die Rede ist. So ist es laut Mitteilung insbesondere erforderlich, bestehende Instrumente zu überarbeiten, um sie an die vorgeschlagene Richtlinie anzupassen. Der EDSB unterstützt diese Absicht vollinhaltlich und fordert die Kommission auf, in diesem Sinne weitere Maßnahmen zu ergreifen.

2.2. Spezifische Kommentare

Bewertung von Instrumenten

25. In der Mitteilung werden einige erfolgreiche Beispiele des Informationsaustauschs nach der schwedischen Initiative und dem Prüm-Beschluss aufgeführt; es wird jedoch gleichzeitig unterstrichen, dass die Anwendung des Prüm-Beschlusses nur sehr schleppend erfolgt und dass die schwedische Initiative ihr volles Potenzial noch nicht erreicht hat. Mit Blick auf die SIS- und SIRENE-Kanäle werden in der Mitteilung keine Empfehlungen ausgesprochen, weil bereits umfassende Veränderungen eingeleitet wurden, insbesondere die Migration zu SIS II.[26]

26. Die Mitteilung besagt, dass die ersten Ergebnisse des Informationsaustauschs gestützt auf die schwedische Initiative und die Prüm-Beschlüsse im Bereich der Strafverfolgung positiv ausfallen. Der EDSB verweist jedoch darauf, dass eine vollständige Bewertung dieser Instrumente (gegebenenfalls einschließlich eventueller Mängel und Schwachstellen der Systeme wie der Anzahl der fälschlicherweise verhafteten oder nach einem falschen Treffer im System belästigten Personen) erst vorgenommen werden kann, wenn sie voll angewandt werden. Er fordert die Kommission auf, mit der Bewertung dieser Instrumente während und nach Abschluss ihrer vollständigen Anwendung fortzufahren.

Wahl der Kanäle

27. In ihrer Mitteilung stellt die Kommission fest, dass die Mitgliedstaaten - abgesehen von den gesetzlichen Vorgaben über die Nutzung bestimmter Kanäle - verschiedene Kanäle in unterschiedlichem Ausmaß nutzen. In der Mitteilung deutet zwar nichts darauf hin, dass die Nutzung verschiedener Kanäle Anlass zu Bedenken gibt, doch kommt die Kommission zu dem Schluss, dass es Zeit für einen kohärenteren Ansatz ist, bei dem Europol eine zentrale Rolle spielen soll. In diesem Zusammenhang fordert die Kommission die Mitgliedstaaten auf, für einen Informationsaustausch, bei dem der Kanal nicht gesetzlich vorgegeben ist, den EUROPOL-Kanal mit SIENA als Standardkanal zu verwenden, sofern keine konkreten Gründe für die Verwendung eines anderen Kanals vorliegen.

[26] Siehe hierzu die Ankündigung der Kommission am 9. April 2013: 'SIS II goes live' : http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130409_01_en.htm

28. Auch der EDSB ist der Ansicht, dass es für die Wahl der Kanäle eines kohärenten und harmonisierten Ansatzes bedarf. Im Hinblick auf die Verwendung eines der Kanäle als Standardkanal erinnert er jedoch an den Grundsatz der Zweckbindung, einen der Kerngrundsätze des Datenschutzes. Wie es in der Mitteilung heißt, gibt es eine Vielfalt von Kommunikationsinstrumenten, -kanälen und -mitteln, die jeweils für bestimmte Zwecke zu verwenden sind. Die Verwendung eines für einen bestimmten Zweck konzipierten Kanals sollte allerdings nicht dazu führen, dass die über diesen Kanal übermittelten Daten möglicherweise für andere Zwecke verwendet oder erhoben werden. Hier besteht ein Risiko, das häufig als „Zweckentfremdung" bezeichnet wird, also eine allmähliche Ausdehnung der Nutzung eines Systems oder einer Datenbank über den Zweck hinaus, zu dem es/sie ursprünglich konzipiert wurde. Die Verwendung eines bestimmten Kanals wirkt sich ferner unmittelbar auf die Verantwortung für Datenschutz und Sicherheit der Behörde/Agentur aus, die den Kanal verwaltet. Der EDSB bedauert, dass in der Mitteilung auf diese Konsequenzen nicht eingegangen wird, und empfiehlt, dass der Rat in dem Leitfaden, den er ausarbeiten soll, diesen Blickwinkel berücksichtigt.

29. Schließlich weist der EDSB noch darauf hin, dass Mechanismen, die für den Informationsaustausch für einen bestimmten Zweck entworfen wurden, nicht unbedingt auch für andere Zwecke geeignet sind. Das von EUROPOL entwickelte Kommunikations-Tool SIENA wurde auf einen bestimmten Informationsaustausch zwischen den zuständigen Behörden von Mitgliedstaaten und Dritten in der polizeilichen Zusammenarbeit zugeschnitten. Spezifische Funktionalitäten von SIENA wurden also aufgrund des Bedarfs entwickelt und umgesetzt, der zum Zeitpunkt der Schaffung dieses Tools bestand. Diese Funktionalitäten verlangen unter anderem von den Verwendern, bestimmte Arten und Mengen von Informationen einzugeben. Der EDSB weist darauf hin, dass die Funktionalitäten von SIENA nicht unbedingt auch für den Informationsaustausch in einem anderen Kontext und für andere Zwecke geeignet sein müssen. In diesem konkreten Fall fordert er daher die Kommission auf, ihre Entscheidung für diesen Kanal besser zu begründen und der Frage nachzugehen, ob diese Entscheidung im Einklang mit dem Grundsatz des eingebauten Datenschutzes steht.

Verwaltung der Kanäle – Nationale Kontaktstelle

30. In der Mitteilung werden die Mitgliedstaaten aufgefordert, eine nationale Kontaktstelle als zentrale Anlaufstelle für die internationale Zusammenarbeit einzurichten bzw., falls bereits vorhanden, zu nutzen, die alle wichtigen Kanäle umfasst, rund um die Uhr in Betrieb ist und alle Strafverfolgungsbehörden mit Zugriff auf alle relevanten nationalen Datenbanken zusammenbringt. In Anbetracht der Tatsache, dass sich auf nationaler Ebene unterschiedliche Stellen mit unterschiedlichen Bereichen der polizeilichen Zusammenarbeit befassen, dürfte nach Auffassung des EDSB der Zugang über eine nationale Kontaktstelle dem ersuchenden Land helfen, da es sich nicht mehr an verschiedene Behörden und Kontaktstellen im ersuchten Landen wenden muss.

31. Die Einrichtung nationaler Kontaktstellen könnte von Vorteil sein, da sie den Überblick über den grenzüberschreitenden Datenfluss erleichtert und eine Aufzeichnung unmittelbar beteiligter Akteure ermöglicht. Bei der Einrichtung

nationaler Kontaktstellen sollten jedoch die datenschutzrechtlichen Implikationen bedacht werden. Alle Datenbanken wurden für genau festgelegte Zwecke aufgebaut und unterliegen besonderen Vorschriften. Zugriff auf eine Datenbank haben nur ordnungsgemäß befugte Mitarbeiter in Wahrnehmung ihrer Aufgaben und für die Zwecke, für die die Datenbank geschaffen wurde. Daher sollten die Zusammensetzung und die Modalitäten nationaler Kontaktstellen sorgfältig geprüft und festgelegt werden, damit gewährleistet ist, dass die für die jeweilige Datenbank geltenden Vorschriften auch eingehalten werden.

32. Solange es keine harmonisierten Bedingungen für nationale Kontaktstellen gibt, könnte es vorkommen, dass in den nationalen Kontaktstellen vertretene Einrichtungen nicht zum direkten Zugriff auf die Datenbank befugt sind, sondern den Zugang ermöglichen und dafür sorgen werden, dass die angeforderten Informationen an die ersuchte Behörde von einem anderen Mitgliedstaat übermittelt werden. Der EDSB hält fest, dass laut Mitteilung die nationalen Kontaktstellen, soweit gesetzlich zulässig, direkten Zugriff auf die nationalen Datenbanken haben sollten. Der EDSB stellt mit Zufriedenheit fest, dass in der Mitteilung daran erinnert wird, dass Informationen tatsächlich nur ausgetauscht und verwendet werden dürfen, wenn dies gesetzlich zulässig ist und wenn damit auch die Datenschutzvorschriften eingehalten werden. Er fordert jedoch die Kommission auf, mit den Arbeiten an harmonisierten Bedingungen für nationale Kontaktstellen zu beginnen und so zu gewährleisten, dass die Anforderungen in allen Mitgliedstaaten ähnlich sind und Personen wirksamen Schutz bieten.

Gewährleistung von Datenqualität, Datensicherheit und Datenschutz

33. Mit Blick auf die Interoperabilität der in der Mitteilung erwähnten verschiedenen nationalen Systeme und Verwaltungsstrukturen unterstreicht der EDSB, dass der Schutz personenbezogener Daten als fester Bestandteil der Herstellung oder Verbesserung der Interoperabilität einschlägiger Systeme gelten muss.

34. Wie bereits in früheren Kommentaren und Stellungnahmen hervorgehoben[27], wird dadurch, dass der Zugang zu oder der Austausch von Daten technisch ermöglicht wird, der tatsächliche Zugang zu diesen Daten bzw. ihr Austausch in vielen Fällen beträchtlich stimuliert. Auch wenn die Herstellung von Interoperabilität nicht zu neuen Datenbanken führen wird, wird sie zwangsläufig eine neue Form der Nutzung bestehender Datenbanken durch neue Möglichkeiten des Zugriffs auf diese Datenbanken mit sich bringen.

35. In diesem Zusammenhang weist der EDSB auf den grundlegenden Datenschutzgrundsatz der Zweckbindung hin, dem zufolge personenbezogene Daten nicht für Zwecke verwendet werden dürfen, die mit dem Zweck unvereinbar sind, für den die Daten ursprünglich erhoben wurden, sofern dies nicht unter besonders strengen Auflagen gestattet ist.

[27] Siehe Stellungnahme des EDSB vom 26. Februar 2006 über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit; Kommentare des EDSB vom 10. März 2006 zur Mitteilung der Kommission vom 24. November 2005 über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen, und Stellungnahme des EDSB vom 7. Dezember 2009 über die Agentur für IT-Großsysteme.

Verbesserung der Fortbildung und Sensibilisierung

36. In der Mitteilung wird erwähnt, dass die Kommission ein europäisches Fortbildungsprogramm im Bereich der Strafverfolgung erstellt, in das auch die Vermittlung von Kenntnissen über den grenzüberschreitenden Informationsaustausch aufgenommen werden wird. Der EDSB hält fest, dass die Kommission vor kurzem eine Mitteilung über die Erstellung eines europäischen Fortbildungsprogramms im Bereich der Strafverfolgung[28] angenommen hat, auf die er in seiner Stellungnahme zum Vorschlag für eine Europol-Verordnung[29] eingehen wird. In Anbetracht der Tatsache, dass vom grenzüberschreitenden Informationsaustausch in einer Reihe von Fällen auch personenbezogene Daten betroffen sein werden, weist der EDSB auf die Notwendigkeit hin, in das von der Kommission vorgesehene Programm sowie in die Fortbildungskurse, die die Mitgliedstaaten durchführen sollen, auch Kurse über Informationssicherheit und Datenschutz aufzunehmen.

3. SCHLUSSFOLGERUNGEN

37. Der EDSB schätzt die allgemeine Aufmerksamkeit, die dem Datenschutz in der Mitteilung zuteil wird; dort wird unterstrichen, dass ein hohes Maß an Datenqualität, Datensicherheit und Datenschutz erforderlich ist, und es wird daran erinnert, dass unabhängig von der Kombination oder Sequenz die für jedes Instrument geltenden Regeln zum Datenschutz, zur Datensicherheit und zur Datenqualität sowie die Bestimmungen zur Zweckbestimmung des Instruments einzuhalten sind.

38. Weiter äußert sich der EDSB folgendermaßen:

- Er begrüßt die Schlussfolgerung der Mitteilung, dass weder neue Strafverfolgungsdatenbanken auf EU-Ebene noch neue EU-Instrumente für den Informationsaustausch erforderlich sind;

- er unterstreicht die Notwendigkeit einer gründlichen Sichtung der Instrumente und Initiativen im Bereich Justiz und Inneres, deren Ergebnisse in eine umfassende, integrierte und durchstrukturierte EU-Politik für das Management von Informationen und des Informationsaustauschs einfließen sollten, und er fordert die Kommission auf, mit der Bewertung anderer bestehender Instrumente fortzufahren;

- er fordert die Kommission auf, sich i) Gedanken zu machen über die Wirksamkeit von Datenschutzgrundsätzen im Lichte des technologischen Wandels, die Entwicklungen bei IT-Großsystemen und die zunehmende Verwendung von Daten, die ursprünglich für Zwecke erhoben wurden, die nichts mit der

[28] Mitteilung der Kommission vom 27. März 2013 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über ein Europäisches Fortbildungsprogramm für den Bereich Strafverfolgung, COM(2013) 172 final.

[29] Vorschlag vom 27. März 2013 für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und Fortbildung im Bereich Strafverfolgung (Europol) und zur Aufhebung der Beschlüsse 2009/371/JI und 2005/681/JI, COM(2013) 173 final.

Verbrechensbekämpfung zu tun haben, sowie ii) der Frage nachzugehen, ob der derzeit zu beobachtende Trend zu einer breit angelegten, systematischen und proaktiven Überwachung nicht verdächtiger Personen die öffentliche Sicherheit wirklich verbessert und ob er tatsächlich einen Beitrag zur Bekämpfung der Kriminalität leistet; das Ergebnis dieser Überlegungen sollte eine umfassende, integrierte und durchstrukturierte EU-Politik für das Management von Informationen und des Informationsaustauschs in diesem Bereich sein;

- er unterstreicht, dass die laufenden Diskussionen über den Vorschlag für eine Richtlinie die Kommission nicht davon abhalten sollten, eine Bestandsaufnahme der Probleme und Risiken des Datenschutzes vorzunehmen und sich Gedanken über mögliche Verbesserungen im aktuellen rechtlichen Kontext zu machen, und er empfiehlt, diese Diskussionen insbesondere zu einer klaren Unterscheidung der Verarbeitung von Daten über verdächtige und nicht verdächtige Personen für die weitere Entwicklung des Europäischen Modells für den Informationsaustausch zu nutzen;

- er ist voll und ganz der Auffassung, dass das bestehende Instrumentarium überprüft und an die vorgeschlagene Richtlinie angepasst werden sollte und fordert die Kommission auf, weitere Maßnahmen zu ergreifen;

- er fordert die Kommission auf, mit der Bewertung bestehender Instrumente während und nach ihrer vollständigen Anwendung fortzufahren;

- er empfiehlt, in dem Leitfaden zur Wahl des Kanals, zu dessen Ausarbeitung der Rat aufgefordert wurde, den Folgen für Zweckbindung und Verantwortlichkeiten Rechnung zu tragen;

- er fordert die Kommission auf, die Entscheidung für den Europol-Kanal mit Nutzung von SIENA als Standardkanal besser zu begründen und der Frage nachzugehen, ob diese Entscheidung im Einklang mit dem Grundsatz des eingebauten Datenschutzes steht;

- er stellt mit Zufriedenheit fest, dass in der Mitteilung daran erinnert wird, dass Informationen tatsächlich nur ausgetauscht und verwendet werden dürfen, wenn dies gesetzlich zulässig ist und wenn damit auch die Datenschutzvorschriften eingehalten werden, und er fordert die Kommission auf, mit den Arbeiten an harmonisierten Bedingungen für nationale Kontaktstellen zu beginnen und so zu gewährleisten, dass die Anforderungen in allen Mitgliedstaaten ähnlich sind und Personen wirksamen Schutz bieten;

- er empfiehlt, in das von der Kommission vorgesehene Programm sowie in die Fortbildungskurse, die die Mitgliedstaaten durchführen sollen, auch Kurse über Informationssicherheit und Datenschutz aufzunehmen.

Brüssel, den 29. April 2013
(unterzeichnet)

Peter HUSTINX
Europäischer Datenschutzbeauftragter