Deutscher Bundestag **Drucksache 16/9987**

16. Wahlperiode 15. 07. 2008

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Silke Stokar von Neuforn, Wolfgang Wieland, Manuel Sarrazin, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 16/9874 –

Interoperabilität von Datenbanksystemen im Bereich der Inneren Sicherheit

Vorbemerkung der Fragesteller

Innerhalb des Bundesverwaltungsamtes (BVA) wird seit dem Jahr 2006 an dem Projekt „Reengineering der Plattformen Innere Sicherheit“ (RISP) gearbeitet.

Hintergrund dessen ist, dass nach Mitteilung des Bundesministeriums des Innern (BMI) vom 12. Oktober 2007 die relevanten Datenbanken der Sicherheitsbehörden und Nachrichtendienste des Bundes derzeit aus technischen, organisatorischen und rechtlichen Gründen getrennt gehalten werden und deswegen „relativ unkoordiniert nebeneinander stehen“ würden. Gleichzeitig sei aber absehbar dass deutsche Behörden im Zuge des weiteren Aufbaus einer europäischen Informationsinfrastruktur europäische Datenbanken (wie das Schengener Informationssystem (SIS) bzw. das Visa-Informationssystem – VIS) verstärkt bedienen und nutzen würden.

Allgemeines Ziel des RISP-Projekts ist es demzufolge, wichtige nationale Systeme und Datenbestände der Inneren Sicherheit in eine gemeinsame Plattform zu integrieren und so die behördenübergreifende Zusammenarbeit in diesem Bereich zu fördern.

Mit dieser „Plattform Innere Sicherheit“ soll – zunächst für sog. Fachverfahren des BVA – eine gemeinsame Ebene geschaffen werden, um übergreifende Mechanismen anbieten zu können.

Zu diesen Fachverfahren des BVA gehören

- das Ausländerzentralregister (mit dem Teilverfahren SIS),
- das automatisierte Sichtvermerksverfahren (mit den Bestandteilen Visa Datei, Visa Dezentral und Visa Online),
- der Biometrieserver des BVA sowie
- das VIS.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 14. Juli 2008 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Konkret wird versucht, mit der „Plattform Innere Sicherheit“ u. a. folgende Ziele zu erreichen:

- Bereitstellung aller Dienste der Inneren Sicherheit über eine – aus Sicht der nutzenden Behörden – integrierte Plattform.
- Medienbruchfreie und rechtssichere Bereitstellung aller für den jeweiligen Nutzer rechtlich verfügbaren relevanten Informationen.
- Verbesserte Abfrageergebnisse durch Konsolidierung der Einzelergebnisse zu einem Gesamtergebnis.

Das RISP-Projekt soll in den Jahren 2006 bis 2011 realisiert werden. Ende letzten Jahres sollten z. B. eine sog. Anforderungsanalyse und eine sog. Datenmigrationsstudie fertiggestellt worden sein. Als erster Umsetzungsschritt soll Ende 2008 die sog. erste Migrationsstufe abgeschlossen werden.

Mit dem RISP-Projekt stellt sich die Bundesregierung auf nationaler Ebene der Herausforderung einer verbesserten Interoperationalität verschiedener Datenbestände aus dem Bereich der Inneren Sicherheit. Diese Frage spielt in den letzten drei Jahren aber auch auf europäischer Ebene eine zunehmende Rolle.

In ihrer Mitteilung über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen hatte die EU-Kommission im November 2005 darauf hingewiesen, dass es derzeit nicht möglich sei, asyl-, einwanderungs- und visabezogene Daten für die Belange der Inneren Sicherheit zu nutzen. Sie schlug daher u. a. vor

1. kohärentere Datenkategorien zwischen SIS II, VIS und Eurodac einzuführen sowie
2. eine serviceorientierte Architektur für die europäischen IT-Systeme zu entwickeln, um entweder
   - die Funktionen von Dateien (wie z. B. dem VIS und EURODAC) besser miteinander zu teilen (ohne diese miteinander zu verschmelzen) oder
   - diese Systeme zu einer einzigen organisatorischen Einheit zusammenzuführen (KOM(2005) 597, S. 8 und 11 f.).

Die Bundesregierung begrüßte in ihrer Stellungnahme zwar ganz allgemein die von der Europäischen Kommission vorgeschlagene Berücksichtigung der Interoperabilität bei der Entwicklung computergestützter Datenbanksysteme der EU. Zu den o. g. konkreten Handlungsvorschlägen der Europäischen Kommission (Punkt 5. 1. und 5. 4 der Mitteilung) legte sie sich jedoch nicht fest. Auch erhob sie keinerlei datenschutzrechtliche Bedenken (EU-Ratsdok. 9855/06).

Ganz anders der Europäische Datenschutzbeauftragte (EDPS), Peter Hustinx. Dieser hatte im März 2006 ausführlich und kritisch zu der Mitteilung der Europäischen Kommission Stellung bezogen (EU-Ratsdok. 7660/06). So begrüßt der EDPS zwar ausdrücklich die Absicht die Effizienz der großen Datenbanksysteme der EU zu verbessern. Allerdings warnte er davor, dass Versuche diese europäischen Datenbanken untereinander operabel auszugestalten bzw. diese Datenbanksysteme mit denen der Mitgliedstaaten zu verknüpfen, die Möglichkeit einer wirksamen und kohärenten Datenschutzkontrolle – sowohl auf EU-Ebene, als auch auf der Ebene der Mitgliedstaaten – verringern würde (eine Position, die der EDPS im März 2008 in seinen vorläufigen Anmerkungen zu den Vorschlägen der EU-Kommission für eine Europäische Grenzschutzverwaltung wiederholte; vgl. www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_ EN.pdf)

Der EDPS wies in diesem Zusammenhang u. a. auf die besondere datenschutzrechtliche Bedeutung der sog. Primärschlüssel von Datenbanken hin. Das ist eine eindeutige Kennnummer, die für jede Person bzw. für jedes Objekt erzeugt wird, zu der/dem Informationen gesammelt und gespeichert wer-

den (z. B. die Nummer der Visummarke, die Teil des künftigen VIS sein wird). Dieser Primärschlüssel – so Peter Hustinx – gilt im Zusammenhang mit der Interoperabilität von Datenbanken als entscheidender Punkt. Die gemeinsame Nutzung von Primärschlüsseln kann nämlich beschränkt werden. Dies würde häufig als ein wirksames Instrument für den Datenschutz eingesetzt. Zwar sei Interoperabilität auch unter solchen Umständen möglich, allerdings seien diese Datenaustauschprozesse dann weniger direkt und könnten so datenschutzrechtlich besser überwacht werden.

In diesem Kontext sprach sich Peter Hustinx gegen die Verwendung biometrischer Merkmale als Primärschlüssel aus:

- Zum einen basieren biometrische Merkmale letztlich auf Wahrscheinlichkeiten und seien daher nicht hinreichend zweifelsfrei und eindeutig.
- Zum anderen würde es bei dieser Art von Primärschlüsseln möglich, verschiedene Datenbanken beinahe in Echtzeit und ohne größere Mühe zusammenzuführen.

Peter Hustinx unterschied zudem zwischen einer horizontalen Interoperabilität von Datenbanksystemen (z. B. zwischen IT-Systemen der EU) und einer vertikalen Verknüpfung bzw. Zusammenführung von Datenbanken der EU mit entsprechenden Systemen der Mitgliedstaaten bzw. der Mitgliedstaaten untereinander (wie z. B. beim sog. Prümer Vertrag). Dieser Trend zur vertikalen Verknüpfung würde – so Peter Hustinx – zur Ausbreitung dezentralisierter Datenbankkonstellationen bzw. von Netzwerken führen, in denen die Anwender unmittelbar miteinander kommunizieren. Diesbezüglich warnt Peter Hustinx vor Zweierlei:

- Zum einen erhöht die Zusammenführung von Datenbanken die Gefahr der Zweckentfremdung von Daten, dann nämlich wenn zwei Datenbanken, die zwei unterschiedlichen Zwecken dienen, zu einem dritten Zweck, für den sie nicht konzipiert waren, verknüpft werden.
- Zum anderen bekräftigte Peter Hustinx seine Bedenken, biometrische Merkmale als sog. Primärschlüssel für diese immer größer und unübersichtlicher werdenden Datenbanksysteme zu nutzen.

Besonderes Augenmerk widmete der Europäische Datenschutzbeauftragte im Hinblick auf Fragen der Interoperabilität der Rolle von Sicherheitsbehörden. Denn, wenn den Polizeibehörden und Nachrichtendiensten der Mitgliedstaaten Zugang zu Datenbanken (wie z. B. dem VIS) ermöglicht werden soll (in denen in der Regel Menschen verdachtsunabhängig erfasst werden), dann sollten – so Peter Hustinx – die Zugangsschwellen für diese Sicherheitsbehörden „stets signifikant höher angesetzt sein, als die Schwelle für die Abfrage strafrechtlicher Datenbanken“. Aus diesem Grunde sieht z. B. auch Artikel 3 Abs. 2 der zwischen Rat und dem Europäischen Parlament konsentierten Verordnung zur Errichtung des VIS vor, dass die nationalen polizeilichen Staatsschutzbehörden bzw. die Geheimdienste keinen Onlinezugriff, sondern nur einen über nationale Zentralstellen vermittelten Zugang zum VIS erhalten sollen (vgl. EU-Ratsdok. PE-CONS 3630/07).

In der Arbeit der zuständigen Ratsarbeitsgruppen spielte die o. g. Kommissionsmitteilung übrigens – soweit erkennbar – keine Rolle mehr. Das Thema „Interoperabilität“ taucht seither allerdings in anderem Zusammenhang immer wieder auf:

- So wurde z. B. bei EUROPOL ein „Secure Information Exchange Network Application“ (SIENA) eingerichtet, das als interoperable Kommunikationsplattform zwischen EUROPOL und den Mitgliedstaaten fungieren soll (vgl. EU-Ratsdok. 7801/08 und 7804/08).
- Im Frühjahr 2007 wurden zwischen den nationalen Zentralstellen des SIS mindestens drei Testläufe zur Erprobung der Interoperabilität des SIS durchgeführt (EU-Ratsdok. 7798/2/07).
- In Ljubljana fand im Januar 2008 ein Treffen u. a. des Strategischen Komitees des Rates „Einwanderung, Grenzen und Asyl“ (SCIFA) statt, auf dem über Fragen der Interoperabilität von Datenbanksystemen diskutiert wurde (vgl. EU-Ratsdok. 8759/08).

- Im Mai 2007 wurde in Deutschland eine Konferenz der sog. Chief Information Officers der Polizeibehörden der Mitgliedstaaten mit dem Titel „Interoperability and data exchange between the European Police Forces“ durchgeführt. Auf dieser Konferenz wurden z. B. große Unterschiede in der Hardware bei den jeweiligen europäischen Polizeibehörden bzw. das Fehlen gemeinsamer technologischer Standards festgestellt. Diese sog. technical gaps könnten die Einführung neuer IT-Systeme bei den europäischen Polizeibehörden beeinträchtigen (vgl. EU-Ratsdok. 10063/07). Die amtierende slowenische Ratspräsidentschaft hat nun im März 2008 ein Grundlagendokument mit dem Titel „Interoperability and data exchange between the European Police Forces – Common Requirements Vision“ vorgelegt. Darin wird der Entwurf eines „IT Interoperability Programme of the European Police Forces“ angekündigt. Für ein erneutes Treffen der „Conference of the Chief Information Officers of Police Forces in Europe“ in Schweden im Juni 2008 hatte sich Deutschland bereiterklärt, in dieser Angelegenheit ein Eckpunktepapier sowie eine sog. road map vorzubereiten (EU-Ratsdok. 7758/08).

Vorbemerkung der Bundesregierung

Die Antwort der Bundesregierung bezieht sich auf die gestellten Fragen. Dies bedeutet keine Zustimmung zu dem Text, der dem Fragekatalog vorangestellt ist.

Reengineering der Plattformen Innere Sicherheit

1. Welche Fachverfahren bzw. welche Datenbanksysteme (des BVA oder anderer Bundesbehörden) sollen im Zuge des RISP-Projekts untereinander bzw. im Hinblick auf welche anderen nationalen bzw. welche europäischen Datenbänke hin in welcher Form vernetzt werden?

Bei RISP handelt es sich um ein rein technisches Migrationsprojekt, das die in verschiedenen IT-Anwendungen des BVA vorhandenen Funktionalitäten auf eine neue, zukunftssichere Plattform überträgt. Durch RISP werden keine neuen Vernetzungen von nationalen oder europäischen Datenbanken hergestellt.

2. Welche neuartigen übergreifenden Mechanismen will die Bundesregierung über die Einrichtung einer gemeinsamen Plattform im BVA – bestehend aus dem Ausländerzentralregister (mit den Teilverfahren SIS), dem automatisierten Sichtvermerksverfahren (mit den Bestandteilen Visa Datei, Visa Dezentral und Visa Online), dem Biometrieserver sowie dem VIS – für Anwenderinnen und Anwender welcher Behörden anbieten?

Durch das RISP-Projekt werden keine neuartigen übergreifenden Mechanismen angeboten, da es sich bei RISP um ein rein technisches Migrationsprojekt handelt.

3. Sofern es zutrifft, dass das RISP-Projekt zunächst nur Fachverfahren aus dem das Bundesverwaltungsamt betrifft, ist zu fragen; welche anderen Fachverfahren bzw. welche anderen Datenbanksysteme aus welchen anderen Bundesbehörden plant die Bundesregierung innerhalb welchen Zeitraums analog zum RISP-Projekt zu vernetzen?

Derzeit ist nicht geplant, andere Fachverfahren oder Datenbanksysteme aus anderen Bundesbehörden zu vernetzen.

4. Welche bzw. wie viele derartige Plattformen plant die Bundesregierung?

Derzeit sind keine weiteren vergleichbaren Plattformen bekannt.

5. Welche „Dienste der Inneren Sicherheit“ sollen schlussendlich „über eine aus Nutzersicht integrierte Plattform“ verfügbar sein?

Ziel der vorgesehenen Plattform ist die technische Optimierung der Bereitstellung der heute vom BVA betriebenen Anwendungen (siehe Antwort zu Frage 2).

6. Mit welchen sog. Primärschlüsseln arbeiten die Datenbankssysteme der Bundesbehörden derzeit?

   Inwiefern plant die Bundesregierung hieran etwas strukturell zu verändern (z. B. biometrische Merkmale als Primärschlüssel einzuführen)?

„Primärschlüssel“ wird hier im Sinne eines möglicherweise eingesetzten Suchkriteriums aufgefasst.

Die Voraussetzungen für den Datenabruf aus von der Bundesverwaltung betriebenen Registern sind rechtlich definiert. Die betreibenden Bundesbehörden sind daher verpflichtet, den berechtigten Nutzern den Zugang nach Maßgabe der jeweiligen bereichsspezifischen Bestimmungen zu eröffnen.

Beispielhaft sei auf Artikel 15 Abs. 2 der VIS-Verordnung verwiesen. Danach können Visumbehörden zum Zweck der Antragsprüfung einzeln oder kombiniert mit einer Vielzahl dort näher bestimmter alphanumerischer Daten sowie mit Fingerabdrücken Suchen im VIS durchführen.

Eine Übersicht aller Suchkriterien aller Datenbanksysteme von Bundesbehörden liegt dem Bundesministerium des Innern nicht vor und ist auch in der Kürze der zur Beantwortung zur Verfügung stehenden Zeit nicht zu ermitteln.

Es existieren derzeit keine Planungen der Bundesregierung, an der Art der verwendeten Suchkriterien strukturell etwas zu verändern.

7. Wie bewertet die Bundesregierung die Bedenken des Europäischen Datenschutzbeauftragten im Hinblick auf die Verwendung biometrischer Daten als Primärschlüssel?

Der Europäische Datenschutzbeauftragte führt als Argument gegen biometrische Merkmale als Primärschlüssel an, dass biometrische Merkmale nicht hinreichend zweifelsfrei und eindeutig seien. Zugleich wird angeführt, dass mit biometrischen Merkmalen als Primärschlüssel Datenbanken beinahe in Echtzeit und ohne große Mühe zusammengeführt werden können.

Grundsätzlich wachsen mit der Anzahl der zu unterscheidenden Datensätze in einer Datenbank die Anforderungen an den Primärschlüssel als Ordnungskriterium für die Datensätze. Dies gilt auch für den Fall, dass biometrische Merkmale als Primärschlüssel verwendet werden. Insofern ist die pauschale Aussage, biometrische Merkmale seien nicht hinreichend zweifelsfrei und eindeutig, so nicht haltbar. Durch die Hinzunahme weiterer Merkmale bei der Ableitung des Primärschlüssels kann ggf. die Zweifelsfreiheit und Eindeutigkeit im Rahmen der bestehenden Anforderungen wiederhergestellt werden.

Die Zusammenführung von Datenbanken ist – abgesehen von den rechtlichen Voraussetzungen – nur dann möglich, wenn volle technische Kompatibilität insbesondere zwischen den Primärschlüsseln besteht. Hierfür sind biometrische Merkmale schlechter geeignet als andere mögliche Primärschlüssel (z. B. eindeutige Ordnungsnummern).

8. Wie bewertet die Bundesregierung die Empfehlung des Europäischen Datenschutzbeauftragten, die gemeinsame Nutzung von Primärschlüsseln aus Gründen einer effektiveren Datenschutzkontrolle zu beschränken?

Eine Bewertung dieser Empfehlung des Europäischen Datenschutzbeauftragten muss noch vorgenommen werden. Eine Aussage kann zum jetzigen Zeitpunkt nicht erfolgen.

9. Welche Ressorts bzw. welche Bundesbehörden sind in welcher Form und zu welchem Zweck an dem RISP-Projekt des Bundesverwaltungsamtes beteiligt?

Das BVA hat keine weiteren Bundesbehörden an dem Projekt beteiligt.

10. Ist der Datenschutzbeauftragte der Bundesregierung an dem RISP-Projekt beteiligt?

Wenn ja, in welcher Form?

Wenn nein, warum nicht?

Da die bei RISP geplante rein technische Migration keine datenschutzrechtlich relevanten Veränderungen mit sich bringt, wurde der Datenschutzbeauftragte nicht am RISP-Projekt beteiligt. Im Zusammenhang mit dem Betrieb der Datenbanken und Verfahren auftretende datenschutzrechtliche Fragen werden regelmäßig bei den (Kontroll-)Besuchen des Datenschutzbeauftragten im Bundesverwaltungsamt erörtert.

11. Welche Kosten werden für das RISP-Projekt insgesamt veranschlagt, und welche Kosten hat dieses Projekt bislang verursacht (bitte unter Angabe des Einzelplans, des Kapitels sowie der Titelgruppe beantworten)?

Die folgende Tabelle enthält die verursachten und veranschlagten Kosten für das RISP-Projekt unter Angabe des Einzelplans, des Kapitels sowie der Titelgruppe:

RISP	2006	2007	2008	2009	2010	2011	2012	Summe
06 15 – Titelgruppe 55	Ist	Ist	Planung	Planung	Planung	Planung	Planung	
511 55 – Wartungs-kosten			100 000	405 000	473 000	550 000	768 000	2 296 000
518 55 – Miete								
525 55 – Aus- und Fort-bildung			10 000	25 000	25 000	75 000	150 000	285 000
532 55 – Aufträge und Dienstleis-tungen	2 324 764	2 247 241	1 722 000	3 000 000	3 045 000	1 450 000	700 000	14 489 005
812 55 – Erwerb von DV-Anlagen, Geräten, SW, HW		598 653	400 000	511 000	398 000	250 000	424 000	2 581 653
Summe	2 324 764	2 845 894	2 232 000	3 941 000	3 941 000	2 325 000	2 042 000	19 651 658

12. Wie will die Bundesregierung technisch sicherstellen, dass die unterschiedlichen Zugriffsberechtigungen der Sicherheitsbehörden des Bundes auf nationale und europäische Datenbanken auch in interoperablen Datenbanksystemen bzw. in vertikal zusammengeführten Netzwerken gewährleistet werden?

Die Bundesregierung gewährleistet, dass der Zugang von Sicherheitsbehörden zu interoperablen Datenbanksystemen nur im gesetzlich zulässigen Umfang und Verfahren erfolgen kann. Dies wird sowohl durch technische, als auch durch fachliche und organisatorische Maßnahmen gewährleistet.

13. Welche Bundesbehörde soll als Zentralstelle i. S. von Artikel 3 Abs. 2 der VIS-Verordnung fungieren?

Die Abstimmung zur Einrichtung der zentralen Zugangsstellen innerhalb der Bundesregierung und mit den Ländern ist noch nicht abgeschlossen.

14. Wie will die Bundesregierung technisch sicherstellen, dass deutsche Polizeibehörden und Nachrichtendienste auch nach Abschluss des RISP-Projekts bzw. bei Gewährleistung einer interoperablen Vernetzung mit dem VIS gemäß Artikel 3 Abs. 2 der VIS-Verordnung tatsächlich keinen – d. h. auch keinen de facto – Onlinezugriff auf das VIS erhalten?

Die Bundesregierung wird gewährleisten, dass das in Artikel 4 VIS-Zugangsbeschluss vorgesehene Zugangsverfahren über zentrale Zugangsstellen ordnungsgemäß umgesetzt wird. Ein Online-Zugriff der als zugangsberechtigt benannten Behörden wird durch fachlichorganisatorische Maßnahmen ausgeschlossen werden; dabei wird gleichzeitig gewährleistet werden, dass in dringenden Ausnahmefällen nach Artikel 4 Abs. 2 VIS-Zugangsbeschluss Zugangsanträge von der zentralen Zugangsstelle unverzüglich bearbeitet werden können.

Interoperabilität europäischer Datenbanksysteme

15. Wie ist – nach Kenntnis der Bundesregierung – innerhalb des Rates der Beratungs- bzw. Verfahrensstand im Hinblick auf die Mitteilung der EU-Kommission KOM(2005) 597?

Die Kommissionsmitteilung (KOM(2005) 597) stellt ein Diskussionspapier dar, das Anregungen und Impulse für weitere Überlegungen zur Verbesserung der Nutzung von Datenbanken im Bereich Justiz und Inneres geben soll. Die Mitteilung als solche wurde mehrfach im Artikel-36-Ausschuss (am 11./12. April 2006 und 8. Juni 2006) sowie im Strategischen Ausschuss für Einwanderungs-, Grenz- und Asylfragen (SCIFA, am 14./15. März 2006) ohne abschließende Ergebnisse erörtert. Ferner hat der Ausschuss der Ständigen Vertreter am 28. Mai 2008 die Ad-hoc-Gruppe Informationsaustausch reaktiviert, in der künftig Einzelthemen des Informationsaustauschs im Bereich Justiz und Inneres behandelt werden, wobei ein besonderes Augenmerk dem Aspekt der Interoperabilität gelten wird.

16. Wie bewertet die Bundesregierung die Kritikpunkte des Europäischen Datenschutzbeauftragten an der o. g. Mitteilung der EU-Kommission (z. B. „Verringerung der Möglichkeit einer wirksamen und kohärenten Datenschutzkontrolle – sowohl auf EU-Ebene, als auch auf der Ebene der Mitgliedstaaten“ sowie „Gefährdung des Grundsatzes der Zweckbindung von gespeicherten Daten“)?

Die Bundesregierung ist sich mit dem Europäischen Datenschutzbeauftragten darin einig, dass die Interoperabilität von technischen Systemen zur Verarbei-

tung personenbezogener Daten unter gebührender Beachtung der allgemeinen Datenschutzgrundsätze und insbesondere des Grundsatzes der Zweckbindung personenbezogener Daten umzusetzen ist. Zwischen der Interoperabilität von Systemen und Anforderungen des Datenschutzes besteht jedoch – auch nach Auffassung des Europäischen Datenschutzbeauftragten – kein grundsätzlicher Gegensatz.

Die Bundesregierung hat im Zusammenhang mit der Verbesserung des Informationsaustauschs im Bereich der 3. Säule wiederholt auf die Bedeutung flankierender datenschutzrechtlicher Bestimmungen hingewiesen. Sie hat die Verhandlungen eines Rahmenbeschlusses zum Datenschutz in der 3. Säule unter deutscher Präsidentschaft maßgeblich vorangetrieben und setzt sich für eine rasche Verabschiedung des Rahmenbeschlusses ein, auf den sich der Rat bereits im November 2007 politisch geeinigt hat. Für den vom Europäischen Datenschutzbeauftragten angesprochenen Zugriff der Sicherheitsbehörden auf das Visa-Informationssystem wurde zwischenzeitlich auf europäischer Ebene die Rechtsgrundlage geschaffen. Der Beschluss des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten (VIS-Zugangsbeschluss) enthält insbesondere enge Zweckbindungsregelungen (Artikel 5 ff. VIS-Zugangsbeschluss). Auch der Austausch von DNA- und Fingerabdruckdaten nach dem in den europäischen Rechtsrahmen überführten Prümer Vertrag im sogenannten Hit-/No-Hit-Verfahren unterliegt einem strengen Datenschutzregime.

Die Maßnahmen zur Verbesserung der Interoperabilität durch Schaffung europaweiter Standards für die IT-gestützte Kommunikation sollen dazu dienen, den u. a. durch die oben genannten Maßnahmen bereits geschaffenen rechtlichen Rahmen des Informationsaustauschs effizient nutzen zu können. Eine Abschwächung der datenschutzrechtlichen Bestimmungen und Vorkehrungen, namentlich zur Zweckbindung, ist damit weder beabsichtigt noch zwangsläufig verbunden. Dort, wo sich aus einer Maßnahme der Verbesserung der Interoperabilität aus datenschutzrechtlicher Sicht neue Risiken ergeben können, sind unter Umständen weitere rechtliche und technische Schutzvorkehrungen vorzusehen.

17. Wann wurde bei EUROPOL SIENA eingerichtet?

    a) Welche Bundesbehörden haben Zugang zu dieser interoperablen Kommunikationsplattform?

    b) Welche zusätzlichen Zugangsmöglichkeiten bzw. welche zusätzlichen Recherchemöglichkeiten haben deutsche Bundesbehörden aus der Nutzung von SIENA (Zugang zu welchen zusätzlichen Daten bzw. zu welchen zusätzlichen Datenbeständen von EUROPOL)?

    c) Welche zusätzlichen Zugangsmöglichkeiten bzw. welche zusätzlichen Recherchemöglichkeiten hat EUROPOL über SIENA zu bzw. innerhalb welcher Datenbanken welcher deutschen Sicherheitsbehörden?

SIENA (Secure Information Exchange Network Application) wird das Nachfolgesystem des Nachrichtenaustauschsystems InfoEx. InfoEx ist das bestehende Austauschsystem operativer Daten zwischen den bei Europol angesiedelten Verbindungsbeamten (ELOs) der Mitgliedstaaten (MS) und berechtigten Mitarbeitern der Europol-Abteilungen Serious Crime (SC) und Information Management and Technology (IMT). InfoEx ist seit 1996 in Betrieb. Es besteht vor allem aus technischer Sicht ein Weiterentwicklungsbedarf, der durch SIENA umgesetzt wird. Zusätzlich soll mit SIENA die Anbindung der weiteren berechtigten Behörden an das Europol-Informationssystem (Europol-IS) bzw.

die Übermittlung der Abfragen dieser Behörden an das Europol-IS erfolgen. Für den Zugriff auf die Daten des Europol-IS sind neben Mitarbeitern des Bundeskriminalamts (BKA) auch Mitarbeiter aus allen Landeskriminalämtern berechtigt.

Über SIENA werden zusätzlich die in der Europol-Abfrageverordnung benannten deutschen Behörden einen indirekten Zugriff auf die Daten im Europol-IS erhalten. Hierbei handelt es sich um die Bundespolizei, den Zollfahndungsdienst und ausgewählte Staatsanwaltschaften. Dabei erhalten diese Behörden bei einer Recherche lediglich die Information, ob ein Treffer im Europol-IS vorliegt oder nicht. Im Trefferfall können diese Behörden dann weitere Informationen über die Nationale Stelle (hier BKA) anfordern. SIENA ermöglicht Europol keinen Zugriff auf deutsche Datenbanken. SIENA ist derzeit in der Planungsphase und wird frühestens in 2009 mit ersten Funktionalitäten zur Verfügung stehen.

18. War der Datenschutzbeauftragte der Bundesregierung bzw. der Europäische Datenschutzbeauftragte an der Einrichtung von SIENA beteiligt?

    Wenn ja, in welcher Form?

    Wenn nein, warum nicht?

Das SIENA-System zum Austausch von Informationen zwischen EUROPOL und den Mitgliedstaaten ist noch nicht in Betrieb. Die Gemeinsame Kontrollinstanz (GKI) nach Artikel 24 des EUROPOL-Übereinkommens, der der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als deutsches Mitglied angehört, ist im Frühjahr d. J. von EUROPOL über dieses Projekt mit dem Ziel einer datenschutzrechtlichen Bewertung unterrichtet worden. Eine Arbeitsgruppe der GKI EUROPOL befindet sich derzeit in konstruktiven Beratungen mit EUROPOL über das Projekt.

Eine Zuständigkeit des Europäischen Datenschutzbeauftragten ist für EUROPOL nicht gegeben.

19. Was ist mit der Interoperabilität des SIS beabsichtigt?

Das bis August 2007 betriebene SIS I+ war auf maximal 18 Teilnehmer ausgelegt und somit nicht in der Lage, weitere Mitgliedstaaten anzuschließen. Wegen Verzögerungen bei der Realisierung des SIS II, schlug Portugal Ende 2006 vor, das SIS für weitere Mitgliedstaaten zu erweitern. Bei den hinzukommenden Mitgliedstaaten handelte es sich um Estland, Lettland, Litauen, Malta, Polen, Slowakei, Slowenien, Tschechien und Ungarn. Das als SISone4ALL bezeichnete Projekt bestand darin, den neuen Mitgliedstaaten ein einheitliches nationales N.SIS (nationales System) zur Verfügung zu stellen und sie an das bestehende SIS I+ anzuschließen. Die durchgeführten Interoperabilitätstests bestanden darin, die technische Anbindung der zu integrierenden Mitgliedstaaten nachzuweisen. Im Rahmen dieser Tests wurde beispielsweise der Austausch von E-Mails getestet, um sicherzustellen, dass die Kommunikation der nationalen Verbindungsbüros SIRENEN (Supplementary Information Request at the National Entry) technisch reibungslos gewährleistet ist. Als Testdaten wurden fiktive Daten- und Zahlenkombinationen verwendet. Reale Daten kamen nicht zum Einsatz.

Bei der Anbindung der neuen Mitgliedstaaten in das SISone4ALL wurden keine neuen Daten in das System eingeführt. Auch wurde keine Verbindung zu anderen Datenbanken mit anderen Aufgaben und Dateninhalten geschaffen.

Dies ist auch aktuell weder für das bestehende SISone4ALL noch für das zu entwickelnde SIS II vorgesehen.

a) Welche Ergebnisse brachten die im Frühjahr 2007 durchgeführten Testläufe zur Erprobung der Interoperabilität des SIS?

Die Tests lieferten den Nachweis, dass die neun neu in das SIS I+ zu integrierenden Mitgliedstaaten technisch korrekt an das SIS I+ angeschlossen sind und dass die technische Kommunikation reibungslos funktioniert.

b) Wurden diese Ergebnisse dokumentiert (wenn ja, wo, und wann – wenn nein, warum nicht?)

Das Testergebnis ist in dem EU-Ratsdokument 10226/1/07 REV 1 SIRIS 97 SISTECH 86 SCH-EVAL 109 COMIX 512 vom 12. Juni 2007 dokumentiert.

20. War der Datenschutzbeauftragte der Bundesregierung bzw. der Europäische Datenschutzbeauftragte an der Planung, der Durchführung bzw. der Auswertung dieser SIS-Testläufe beteiligt?

Wenn ja, in welcher Form?

Wenn nein, warum nicht?

Bei den Tests handelte es sich lediglich um solche auf technischer Verbindungsebene. Echtdaten wurden in diesem Zusammenhang nicht verwendet. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wurde deshalb mit der Planung, Durchführung und Auswertung dieser Testläufe nicht befasst. Allerdings wurde im Rahmen der Schengen-Evaluierung der neun neuen Mitgliedstaaten eine Überprüfung der Systeme auch speziell unter dem Aspekt des Datenschutzes durchgeführt.

Der Europäische Datenschutzbeauftragte ist für das SIS in seiner aktuellen Form nicht zuständig.

21. War das Treffen im Januar 2008 in Ljubljana, bei dem über Fragen der Interoperabilität von Datenbanksystemen diskutiert wurde, das erste seiner Art, und wenn nein, wann haben hierzu bereits Treffen zu welchen Themen stattgefunden?

a) Über welche Fragen der Interoperabilität welcher Datenbanksysteme wurde auf dem Treffen in Ljubljana debattiert?

b) Wer war auf diesem Treffen vertreten?

c) Welche Ergebnisse brachte dieses Treffen?

d) Wurden diese Ergebnisse dokumentiert (wenn ja, wo, und wann – wenn nein, warum nicht?)

e) Wurden Folgetreffen vereinbart, und wenn ja, für wann, und wo?

Bei dem Treffen am 17./18. Januar 2008 in Ljubljana handelt es sich um ein gemeinsames Seminar des Artikel-36-Ausschusses und des Strategischen Ausschusses für Einwanderungs-, Grenz- und Asylfragen (SCIFA). Es war das bisher erste Treffen dieser Art, bei dem das Thema Interoperabilität diskutiert worden ist. Bei dem Treffen waren alle EU-Mitgliedstaaten und die Kommission vertreten. Das Gespräch diente der Beratung und dem Austausch von Einschätzungen und Positionen, ohne zu abschließenden Ergebnissen zu führen.

Die Beratungen hatten die Themen VIS, Vertrag von Prüm, SIS, Entry/Exit-System, zentrales EU-Fingerabdrucksystem (AFIS), Einführung eines weit-

gehend technikorientierten Grenzkontrollsystems (ETA) sowie die Entwicklung einer langfristig angelegten IT-Strategie für die Europäische Union zum Inhalt. Die Diskussion ergab eine Präferenz dafür, dass vor der Einführung von neuen Systemen zunächst eine Evaluierung stattfinden solle, um etwaige Synergieeffekte zu erreichen. Die Erarbeitung von gemeinsamen IT-Standards zur Erreichung von Interoperabilität seien wichtige Elemente einer zukunftsgerichteten Strategie.

Wegen des informellen Charakters der Sitzung fand eine Dokumentation der Ergebnisse nicht statt. Folgetreffen wurden nicht vereinbart.

22. War der Europäische Datenschutzbeauftragte an der Planung, der Durchführung bzw. der Auswertung dieses Treffen in Ljubljana beteiligt?

    Wenn ja, in welcher Form?

    Wenn nein, warum nicht?

Eine Beteiligung des Europäischen Datenschutzbeauftragten erfolgte mangels Zuständigkeit desselben nicht.

23. Eckpunkte welchen Inhalts will die Bundesregierung dem Treffen der „Conference of the Chief Information Officers of Police Forces in Europe“ im Juni 2008 in Schweden im Hinblick auf den Entwurf eines „IT Interoperability Programme of the European Police Forces“ vorschlagen?

Das Treffen der „Conference of the Chief Information Officers (CIOs) of Police Forces in Europe“ fand am 17. und 18. Juni 2008 in Stockholm statt. Dort wurde diskutiert, dass sich ein „IT Interoperability Programme“ mit organisatorischen Aspekten, einem Anforderungs- und Portfolio-Management und einem Informationsmodell der europäischen Polizeien befassen solle.

Organisatorische Aspekte beziehen sich hierbei z. B. auf die Finanzierung, auf eine enge Abstimmung mit polizeilich-fachlichen Anforderungen, auf eine Einbindung in die regulären EU-Entscheidungsstrukturen sowie auf den organisatorischen Rahmen für die diesbezüglichen Verhandlungen der CIOs.

Ein Anforderungs- und Portfolio-Management soll die Koordination sowohl zwischen fachlicher (polizeilicher) Anforderung und technischer Umsetzung als auch zwischen den verschiedenen laufenden Aktivitäten untereinander (z. B. Projekte SIS II und Vertrag von Prüm, „Schwedische Initiative“ und „Prinzip der Verfügbarkeit“) sicherstellen.

Ein Informationsmodell der europäischen Polizeien soll dem Zweck dienen, dass Anforderungen von technischer Unterstützung (also u. a. die Entwicklung von IT-Systemen bzw. IT-Diensten) nach der rechtlichen Klärung und der politischen Entscheidung zu ihrer Umsetzung mit geringerem Aufwand im jeweiligen Einzelfall umgesetzt werden können. Nicht vorhandene „Rahmenentscheidungen“ (so fehlt z. B. ein einheitliches Informationsmodell, so dass für SIS, Europol-IS und Vertrag von Prüm jeweils eigene Informationsmodelle erstellt wurden) müssen derzeit in jedem Einzelfall verhandelt und entschieden werden. Als Konsequenz werden häufig analoge Fragestellungen immer wieder und unabhängig voneinander behandelt, so dass sich die gestellten Anforderungen nur unter massiven Zeitverlusten und mit erheblichen finanziellen Mehraufwänden erfüllen lassen.

24. Wie soll die von Deutschland vorzubereitende diesbezügliche sog. road map aussehen?

Als Diskussionsgrundlage wurde in der Konferenz vorgeschlagen, ein „IT Interoperability Programme“ in drei Phasen aufzuteilen. In der Vorbereitungsphase müssen im Wesentlichen der Status quo erfasst werden sowie Umfang und Ziele des Programms abgestimmt werden. Hinzu kommt die Klärung organisatorischer Aspekte (siehe Antwort zu Frage 23). Die Pilotphase konzentriert sich auf die Klärung der Rahmenentscheidungen und die Durchführung erster Pilotprojekte. Der Schwerpunkt der Abschlussphase sollte auf dem konsequenten Zusammenführen der verschiedenen Teile des Programms sowohl untereinander als auch mit Initiativen außerhalb des Programms („Konvergenz“) liegen. Dieser Ansatz wurde im Grundsatz positiv aufgenommen. Eine detailliertere Ausarbeitung einer „road map“ hängt jedoch von dem Vorhandensein eines organisatorischen Rahmens für die Ausarbeitung der Punkte des Programms ab (siehe Antwort zu Frage 23).

25. Welche Empfehlungen will die Bundesregierung aus ihrem Programm „Reengineering der Plattformen Innere Sicherheit“ in diesen Prozess einspeisen?

Die Erkenntnisse aus dem Programm „Reengineering der Plattformen Innere Sicherheit“ werden zum Know-how-Transfer und zur Steigerung der Effizienz sukzessive in den Prozess eingebracht. Dies ist maßgeblich vom Fortschritt der Migration abhängig.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333