Deutscher Bundestag **Drucksache 16/9874**

16. Wahlperiode 27. 06. 2008

Kleine Anfrage

der Abgeordneten Silke Stokar von Neuforn, Wolfgang Wieland, Manuel Sarrazin, Volker Beck (Köln), Dr. Uschi Eid, Jerzy Montag, Irmingard Schewe-Gerigk, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Interoperabilität von Datenbanksystemen im Bereich der Inneren Sicherheit

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.

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 11f).

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 werden (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 die 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 „Inter-

operability 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).

Wir fragen die Bundesregierung:

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?
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?
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?
4. Welche bzw. wie viele derartige Plattformen plant die Bundesregierung?
5. Welche „Dienste der Inneren Sicherheit“ sollen schlussendlich „über eine aus Nutzersicht integrierte Plattform“ verfügbar sein?
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)?
7. Wie bewertet die Bundesregierung die Bedenken des Europäischen Datenschutzbeauftragten im Hinblick auf die Verwendung biometrischer Daten als Primärschlüssel?
8. Wie bewertet die Bundesregierung die Empfehlung des Europäischen Datenschutzbeauftragten, die gemeinsame Nutzung von Primärschlüsseln aus Gründen einer effektiveren Datenschutzkontrolle zu beschränken?
9. Welche Ressorts bzw. welche Bundesbehörden sind in welcher Form und zu welchem Zweck an dem RISP-Projekt des Bundesverwaltungsamtes beteiligt?
10. Ist der Datenschutzbeauftragte der Bundesregierung an dem RISP-Projekt beteiligt?

    Wenn ja, in welcher Form?

    Wenn nein, warum nicht?

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

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?
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“)?
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?
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?
19. Was ist mit der Interoperabilität des SIS beabsichtigt?
    a) Welche Ergebnisse brachten die im Frühjahr 2007 durchgeführten Testläufe zur Erprobung der Interoperabilität des SIS?
    b) Wurden diese Ergebnisse dokumentiert (wenn ja, wo, und wann – wenn nein, warum nicht?)
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?

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?

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?

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?

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

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

Berlin, den 26. Juni 2008

Renate Künast, Fritz Kuhn und Fraktion

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