Anfrage

der Abgeordneten Mag. Johann Maier
und GenossInnen
an den Bundeskanzler
betreffend „Biometrie – Hochsicherheitspässe: Einführung – Sicherheit – Datenschutz – Kosten – Nutzen?“

Der Rat der Europäischen Union hat bereits am 13. Dezember 2004 die EU-Verordnung EG 2252/2004 verabschiedet und die Aufnahme eines digitalen Gesichtsbildes und Fingerabdrücke als biometrische Merkmale in den elektronisch lesbaren europäischen Reisepässen ab 2006 bzw. 2008 beschlossen. Diese Entscheidung wurde durch den Europäischen Rates der Regierungsvertreter entgegen der Stellungnahme des Europäischen Parlaments getroffen. Gemäß Art 6 der VO 2252/04 sind die Mitgliedsstaaten zur Integration von biometrischen Merkmalen binnen einer 18- und 36 Monatsfrist nach Notifizierung der technischen Spezifikationen (Verschlüsselungstechnik) durch die Europäische Kommission verpflichtet.
Die biometrischen Merkmale sollen auf einem kontaktlosen Chip gespeichert werden. Vorerst soll das digitale Bild des Passinhabers und der maschinenlesbare Teil (MRZ) auf diesem Chip gespeichert werden, Fingerabdrücke sollen in der EU später hinzukommen (im nicht interoperablen Format). Weltweit ist daher nur das Passbild notwendig, um die Interoperabilität zu gewährleisten (Digitalisierung mit jpeg). Das Bild wird digital gespeichert und angeblich durch eine digitale Signatur verschlüsselt.

Öffentliche Diskussionen darüber fanden in den EU-Mitgliedstaaten bzw. in deren nationalen Parlamenten zur Einführung von Hochsicherheitspässen - insbesondere zur Kosten-Nutzen Frage – bislang kaum statt!

Trotz technischer Mängel (z.B. Biometrische Verfahren) und ungeklärter datenschutzrechtlicher Probleme beabsichtigte die österreichische Bundesregierung allerdings noch in diesem Jahr Reisepässe mit biometrischen Daten (vorerst ohne digitalem Fingerabdruck) einzuführen. Presseberichten zufolge soll diese Einführung nun erst 2006 erfolgen.

Es gibt in Österreich (vermutlich sogar in allen EU-Mitgliedsstaaten) kein umfassendes **Datenschutz- und IT-Konzept** für die so genannten Hochsicherheitspässe: Ein technisches Sicherheitskonzept (Sicherheitsstandards) zum Schutz der im RFID-Chip gespeicherten biometrischen Daten der Passinhaber fehlt.
Dies wurde auch durch einen Beschluss des Europäischen Parlaments (EP) bestätigt:
Es fehlen europaweit verbindliche Mindestanforderungen für biometriegestützte Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und Manipulation der Daten!

Bei einer zehnjährigen Gültigkeit von Reisepässen kann überdies heute niemand ernsthaft ausschließen, dass die Daten durch Sensoren unbemerkt gelesen, kopiert oder verändert sowie missbräuchlich verwendet werden. Das war auch Teil des Ergebnisses einer kürzlich vorgelegten Studie des „Bundesamtes für Sicherheit in der Informationstechnik", immerhin eine nachgeordnete Behörde des deutschen Bundesinnenministeriums.

Auch die damit verbundenen finanziellen Belastungen für den Bund, die einzelnen Passbehörden und die PasswerberInnen sind nicht geklärt. Zu befürchten ist, dass die Passbehörden und die PasswerberInnen die dadurch entstehenden Systemkosten und Mehrkosten zu tragen haben.
Die Budgetanfrage von Abg. Mag. Johann Maier nach den Mehrkosten wurde von der BM für Inneres am 21. März 2005 wie folgt beantwortet:
„Es sind mit Mehrkosten für das Passbuch, die Integration des Chips und die Einbringung der Daten des Antragstellers in das Passbuch sowie auf den Chip zu rechnen.
Diese Kosten wirken sich auf den von den Passbehörden zu entrichtenden Preis des Passes aus."

Zur Zeit nimmt international die Kritik an der kurzfristig beabsichtigen Einführung dieser sogenannten Hochsicherheitspässen mit biometrischen Merkmalen zu. Neben der generellen Sinnhaftigkeit von derartigen Hochsicherheitspässen wurden in den letzten Wochen und Monaten u.a. allfällige Risken, RFID-Chip, Fälschungssicherheit, Datenintegrität, Datenverknüpfung, Gültigkeitsdauer, Kosten und Wartefristen für Passausstellung diskutiert.
Die Erfassung und Verwendung biometrischer Daten muss in Österreich überdies auch im Zusammenhang mit dem „Erkennungsdienst Neu" des BMI gesehen werden (Erkennungsdienstliche Datenbank sowie Digitale Gesichtsdatenbank).

Der deutsche Bundesbeauftragte für Datenschutz, Peter Schaar, hat daher mehr Zurückhaltung bei der Speicherung von Daten gefordert. Angesichts rasanter technologischer Entwicklungen und zunehmender Regeln zum Schutz der inneren Sicherheit äußerte Schaar am 19.04.2005 den Wunsch, „dass der Datenschutz ernster genommen wird". Er forderte ein Moratorium, die Einführung von Hochsicherheitspässen soll in Deutschland um ein Jahr verschoben werden. So könnte die Zeit genützt werden, an der Ausreifung der Technik zu arbeiten, die oft nicht so zuverlässig funktioniere wie angenommen, so Schaar. Es müsse zu einer transparenten Abwägung von Kosten und Nutzen biometrischer Systeme kommen.

Hochsicherheitspässe mit einem oder mehreren biometrischen Merkmalen führen nicht automatisch zu einer Verbesserung der Sicherheit (Konferenz der deutschen Datenschutzbeauftragten am 1. Juni 2005).
Tests haben bewiesen, dass biometrische Identifikationsverfahren einerseits hohe Falscherkennungsraten aufweisen und andererseits oft mit einfachsten Mitteln zu überlisten sind. **Diese scheinbar sicheren Pässe werden durch die derzeitigen unsicheren biometrischen Verfahren zum Sicherheitsrisiko!**

Besonders kritisch wird von Konsumenten- und DatenschützerInnen der Einsatz von RFID-Chip´s gesehen. Laut der gültigen EU-Verordnung sollen die europäischen Reisepässe und Dokumente als Speichermedium einen RFID-Chip enthalten. RFID-Systeme bergen aber derzeit noch eine Vielzahl ungelöster Risiken (Verfälschen der Daten, Abhören der Funksignale, Störung des Datenaustausches etc.). Dies ergibt sich auch aus der inneramerikanischen Diskussion. Bürgerrechtsgruppen, High-Tech-Firmen und die Reisebranche haben Bedenken gegen Teile dieser Technologie, vor allem gegen RFID. Die Funktechnik gilt als unsicher.
Dieser Chip ermöglicht ein berührungsloses Lesen der Reisepassinformation und möglicherweise damit auch eine flächendeckende Überwachung von PassinhaberInnen. Wer über entsprechende Lesegeräte verfügt kann dann damit einerseits öffentliche wie private Räume überwachen, andererseits aber auch die Menschen selbst. Die informationelle Selbstbestimmung ist damit am Ende.

Vorerst kam zur Einführung von Hochsicherheitspässen viel Druck auch von den USA (Patriot act), die Einreisebestimmungen wurden verschärft:

Diese gelten seit 26.Juni 2005, grundsätzlich wird nun ein maschinenlesbarer Pass benötigt. Nach der ursprünglichen US-Vorgabe hätten nach dem 26.Oktober 2005 ohne Visum nur die Person in die USA reisen dürfen, die über einen maschinenlesbaren Pass mit einem biometrischen Kennzeichen verfügen. Der von der EU angestrebten Fristverlängerung bis 2006 wurde nun durch die amerikanische Administration zugestimmt.
Nur wer einen so genannten Hochsicherheitspass besitzt, darf nach dem 31.Oktober 2006 ohne Visum in die USA einreisen. Verlangt wird dafür ein maschinenlesbarer Pass mit einem biometrischen Datum (Visa-Waiver-Programm).

Mit Stichtag 1.September 2006 sollen Pässe mit einem biometrischen Kennzeichen in allen Mitgliedsstaaten der EU eingeführt werden. Eine frühere Einführung obliegt den Mitgliedsstaaten. Die USA selbst planen die Einführung von Pässen mit nur einem biometrischen Merkmal (Gesichtsfeld) nicht vor 2007!

Biometrie wird überdies zunehmend auch durch Unternehmen insbesondere bei der Zugangskontrolle verwendet. So planen beispielsweise einige Airlines ein neues Kontrollsystem mit biometrischen Informationen einzuführen. Diese sind allerdings höchst umstritten.

Die unterzeichneten Abgeordneten richten daher an den Bundeskanzler nachstehende

Anfrage:

1. Sind Sie bereit – insbesondere aus datenschutzrechtlichen Gründen – zumindest einem Moratorium (d.h. einem Aufschub der Einführung der sogenannten Hochsicherheitspässe in Österreich bis zumindest Oktober 2006) zuzustimmen? Wenn nein, warum nicht?

2. Ab welchem Zeitpunkt soll es aus Sicht des Bundeskanzleramtes diese sog. Hochsicherheitspässe mit beiden biometrischen Merkmalen in Österreich geben?

3. Werden Sie in Österreich für einen Großversuch (bzw. zumindest ein Probelauf wie bei der e-card) zu Datenschutz und Datensicherheit, Zuverlässigkeit und

Fehleranfälligkeit biometrischer Systeme vor der Einführung und Ausgabe von elektronisch lesbaren biometrischen Hochsicherheitspässen eintreten? Wenn nein, warum nicht?

4. Wie begründen Sie die Ver- bzw. Anwendung von biometrischen Merkmalen (Daten) in den sog. Hochsicherheitspässen?
   Worin besteht der zusätzliche Sicherheitsnutzen von biometrischen Merkmalen in diesen Pässen?

5. Halten Sie die derzeit in Anwendung befindlichen biometrische Verfahren aus Datenschutzgründen zu Hundertprozent einsatzbereit? Wenn ja, welche Erkenntnisse liegen dem Ressort diesbezüglich vor?

6. Welche wissenschaftlichen Erkenntnisse hinsichtlich der Bewertung biometrischer verfahren liegen dem Bundeskanzleramt vor?

7. Welche Stellungnahmen wurden von Österreich zur Einführung von sogenannten Hochsicherheitspässen auf europäischer Ebene (z.B. EU-Ministerrat) hinsichtlich Datenschutz und Datensicherheit sowie Grundrechtsfragen abgegeben?

8. Auf welche Grundlagen haben die österreichischen Vertreter im Rat ihre Entscheidung für die Einführung biometrischer Merkmale in Pässen und sonstigen Reisedokumente von EU-Bürger gestützt?

9. Aus welchen Gründen haben die österreichischen Vertreter im Rat am 13. Dezember 2004 der EU-Verordnung EG 2252/2004 im Rat zugestimmt, ohne vorher den Nationalrat damit zu befassen?

10. Ist Ihnen bekannt, dass die Art 29 Datenschutzgruppe – in der Österreich vertreten ist – vor diesem Beschluss massive Bedenken gegen die Einführung biometrischer Merkmale in Pässen geäußert hat? Wenn ja, warum haben die Vertreter der österreichischen Bundesregierung – insbesondere Sie als für den Datenschutz ressortzuständiger Bundesminister – im Rat diese Bedenken nicht

berücksichtigt?

11. Werden Sie für die Zweckbindung biometrischer Daten im österreichischen Passgesetz eintreten? Wenn nein, warum nicht?

12. Wie sieht das österreichische Datenschutz- und IT-Sicherheitskonzept bei diesen so genannten Hochsicherheitspässen aus?

13. Welche konkrete Sicherheits- oder Schlüsseltechnik kommt in den österreichischen Hochsicherheitspässen zur Anwendung, damit die digitalen Passdaten weder gelesen noch manipuliert werden können?

14. Welche technische Sicherheitsinfrastruktur ist vorgesehen? Wie bewertet das Bundeskanzleramt den hierzu notwendigen Forschungsbedarf, um etwa kryptographische Sicherheitsmethoden auf Basis kostengünstiger passiver RFID-Chips zu implementieren?

15. Wie wird in Österreich bzw. in allen EU-Mitgliedsländern sichergestellt, dass die sogenannten Hochsicherheitspässe, die mit den richtigen biometrischen Merkmalen (z.B. Gesichtsbild und/oder Fingerabdrücke) des Passinhabers versehen sind, nicht mit falschen Personendaten versehen werden?

16. Wie wird in Österreich bzw. in allen EU-Mitgliedsländern sichergestellt, dass die sogenannten Hochsicherheitspässe, die mit den richtigen Personendaten versehen sind, nicht mit falschen biometrischen Merkmalen versehen werden?

17. Können nach Einführung dieser sogenannten Hochsicherheitspässe (mit einem biometrischen Merkmal) Verbrecher oder Terroristen an der Einreise nach Europa oder Österreich gehindert werden?

18. Ist es richtig, dass die digitalen Passbilder für die sogenannten Hochsicherheitspässe von gewerblichen Photographen über das Internet online an die befasste Passamtbehörde oder die ÖSD übermittelt werden sollen?

19. Wenn ja, wie wird aus Sicht des Bundeskanzleramt bei dieser Übermittlung Datenschutz und Datensicherheit (Datenintegrität) gewährleistet?

20. Ist es richtig, dass die sogenannten Hochsicherheitspässe in Zukunft von der ÖSD mit der Post den PasswerberInnen zugestellt werden?
Wenn ja, wie wird damit – ohne Identitätskontrolle - die Zustellung an den tatsächlichen Antragsteller sichergestellt?

21. Ist es richtig, dass in den sogenannten Hochsicherheitspässen ein kontaktloser RFID-Chip (Funk-Chip) eingesetzt wird? Wie groß ist die Speicherkapazität des vorgesehenen RFID-Chip?

22. Ist es richtig, dass ein digitales Gesichtsbild (und später auch Fingerabdrücke) als biometrisches Kennzeichen auf diesem RFID-Chip (Funkchip) gespeichert werden soll? Wenn nicht, wo dann?

23. Ist es richtig, dass der Chip so gebaut sein muss, dass ein weiteres drittes biometrisches Merkmal (z.B. Iris) gespeichert werden kann?

24. Besteht durch die Möglichkeit des kontaktlosen Auslesens tatsächlich ein Sicherheitsgewinn oder sind hiermit nicht tatsächliche neue Risiken des unbefugten Aus- bzw. Mitlesens zu befürchten? Wie verhalten sich diese Risiken zum Grundrecht auf Datenschutz?

25. Aus welchen Gründen wurde gerade diese Form der Datenübertragung gewählt?

26. Wie wird bei dem nun in Österreich geplanten biometrischen Erkennungsverfahren Datenschutz und Datensicherheit (IT-Sicherheit) garantiert?

27. Sind Ihnen die Berichte bekannt, dass bei Tests mehrere biometrischen Verfahren die angestrebte Sicherheit nicht garantiert haben und die Rate der Falschzurückweisungen, (d. h. die Fälle, in denen das System einen Berechtigten zu Unrecht zurückgewiesen hat), besonders hoch gewesen sind?

28. Was passiert bei einer fehlerhaften Datenübertragung oder Zurückweisung?

29. Wer haftet für den entstandenen Schaden (z.B. Urlaub) bei einer Zurückweisung an einer Grenzkontrollstelle, die auf einen technischen Mangel (z.B. Lesegerät) zurückgeführt wird? Sollen in derartigen Fällen Schadenersatzansprüche gestellt werden können? Wenn nein, warum nicht?

30. Sehen Sie den Chip als Sicherheitsmerkmal?
    Wenn ja, ist dieser fälschungssicher?

31. Welche sonstigen Sicherheitsmerkmale sollen diese sogenannten Hochsicherheitspässe in Österreich enthalten?

32. Ist es richtig, dass die bisher im Pass aufgedruckten Informationen, wie beispielsweise Name, Geburtsdaten, Gültigkeitsdauer und Passnummer zusätzlich auch im Chip gespeichert sind?

33. Ist auf dem RFID-Chip eine Verschlüsselung der erfassten biometrischen Daten und der sonstigen Daten möglich?

34. Wenn ja, wird diese Verschlüsselung vorgenommen?

35. Wie und wodurch wird der in den sogenannten Hochsicherheitspässen verwendete Chip vor unberechtigtem Auslesen ohne Zustimmung und Wissen geschützt (Skimming)?

36. Selbst wenn nach derzeitigem Stand der Technik ein unberechtigtes Mit- bzw. Auslesen nicht möglich sein sollte: Wie ist die langfristige informationstechnische Sicherheit der hierzu eingesetzten Verschlüsselungsverfahren zu bewerten?

37. Können Sie ausschließen, dass die Kommunikation zwischen dem RFID-Chip und dem Lesegerät (z.B. am Flughafen) durch Dritte abgehört werden kann?

38. Können Sie ausschließen, dass mit RFID-Chip´s in sogenannten Hochsicherheitspässen Bewegungsprofile von Passinhabern durch Dritte erstellt werden?

39. Wie sicher sind RFID-Chips gegenüber externer Störquellen?
Wie wird technisch sichergestellt, dass nicht Störsender (z.B. an Grenzkontrollstellen) das behördliche Auslesen der im Chip enthaltenden Daten verhindern?

40. Wie soll sichergestellt werden, dass nur berechtigte Stellen (Behörden) und zwar nur mit Zustimmung des Inhabers des Passes auf die Passdaten zugreifen können, wenn es doch nur eine Frage der Zeit ist, wann der entsprechende Code „gehackt" werden kann?

41. Wann und unter welchen Voraussetzungen erfolgt eine Aktivierung des RFID-Chips?
Wie und unter welchen Voraussetzungen erfolgt die Deaktivierung?

42. Ist es richtig, dass der Chip nicht lesbar d.h. inaktiv ist, solange die maschinenlesbare Zeile (MRZ) nicht benutzt wird?

43. Ist es richtig, dass der Chip erst durch Auflegen auf ein Lesegerät (10 cm über das Lesegerät) durch das Einlesen der MRZ aktiviert und lesbar wird, da die MRZ einen Schlüssel enthält, der erst den Zugriff ermöglicht wird und erst dann Daten übermittelt werden?

44. Welche gutachterlichen Erkenntnisse und Beweise liegen Ihnen vor, dass der „Chip" tatsächlich erst mit dem Einlesen der maschinenlesbaren Teile aktiviert wird?

45. Stellt die MRZ eine Erhöhung der Fälschungssicherheit dar, nachdem das Dokument 9303 (das die Gestaltung des Passes, den Aufbau der MRZ und deren Lesbarkeit regelt) allgemein zugänglich ist und sich die Inhalte der MRZ über das Internet abrufen lassen?

46. Ist es richtig, dass es mit der Einführung der maschinenlesbaren Zeile (MRZ) um eine Beschleunigung der Grenzkontrolle bzw. der Personenabfertigung (Ein- bzw. Ausreise) geht und nicht um eine Erhöhung der Fälschungssicherheit?

47. Können Sie ausschließen, dass durch diese sogenannten Hochsicherheitspässe sowie mit den damit verbundenen zentralen Speichermöglichkeiten und Verknüpfungsmöglichkeiten von biometrischen Daten mit anderen Daten(beständen) „Gläserne Bürger" geschaffen werden können?

48. Dürfen die in Zukunft an den österreichischen Grenzkontrollstellen oder Flughäfen gelesenen biometrischen Passdaten (bei Ausreise oder Einreise) aus datenschutzrechtlicher Sicht in Österreich gespeichert und verwendet werden? Wenn ja, aufgrund welcher Rechtsgrundlage und zu welchen Zwecken?

49. Dürfen in Zukunft die an nicht österreichischen Grenzkontrollstellen oder Flughäfen anderer Mitgliedsstaaten gelesenen biometrischen Passdaten (bei Ausreise oder Einreise) aus datenschutzrechtlicher in diesen Staaten gespeichert und verwendet werden? Wenn ja, aufgrund welcher Rechtsgrundlage und zu welchen Zwecken?

50. Dürfen die an österreichischen Grenzkontrollstellen und Flughäfen gelesenen biometrischen Passdaten (Ausreise oder Einreise) aus datenschutzrechtlicher Sicht mit den in zentralen Datenbanken gespeicherten Daten des BMI u.a. (Erkennungsdienstliche Datenbank oder digitale Bilddatenbank) abgeglichen werden? Wenn ja, mit welchen zentralen Datenbanken oder Referenzdatenbanken und aufgrund welche Rechtsgrundlage?

51. Wenn nein, wird durch das BKA die Auffassung geteilt, dass aus verfassungsrechtlichen Gründen die biometrischen Daten in der Verfügungsgewalt der PassinhaberInnen verbleiben müssen und daher ausschließlich auf dem Reisepass, nicht aber in zentralen Datenbanken gespeichert werden oder mit Referenzdatenbanken abgeglichen werden dürfen?

52. Können Sie in Österreich einen Abgleich der gespeicherten biometrischen Passdaten mit zentralen Datenbanken ausschließen? Wenn nein, warum nicht?

53. Welche staatlichen Stellen (Behörden) in Österreich sollen Zugriff auf die für die Hochsicherheitspässe erfassten biometrischen Daten (digitale Lichtbilddatei oder Fingerabdruckdatei) bekommen?

54. Ist es geplant, anderen Mitgliedsstaaten der EU oder überhaupt anderen Staaten einen Zugriff auf die für die österreichischen Hochsicherheitspässe erfassten biometrischen Daten (Digitale Gesichtsbilddatei und Fingerabdruckdatei) zu gewähren?

55. Wenn ja, aus welchen Gründen und aufgrund welcher Rechtsgrundlage?

56. Unterstützen Sie die Forderung des EU-Parlaments, alle Behörden und sonstige Stellen in ein Register aufzunehmen, die Zugang zu den in den Hochsicherheitspässen im integrierten Chip gespeicherten Daten haben, damit die notwendige Transparenz erreicht und Missbrauch weitgehend vermieden wird? Wenn nein, warum nicht?

57. Werden Sie weiterhin auf europäischer Ebene mit Nachdruck gegen die Einführung einer zentralen europäischen Passdatenbank – die allen biometrischen Daten der EuropäerInnen enthalten würde - eintreten?

58. Welche EU-Mitgliedsländer treten zur Zeit weiterhin für die Einführung einer zentralen europäischen Passdatenbank ein?

59. Welchen konkreten Beitrag können diese geplanten Hochsicherheitspässe mit biometrischen Merkmalen zur Bekämpfung der (organisierten) Kriminalität insbesondere des Terrorismus in Österreich, in der EU bzw. weltweit leisten?

60. Wie sieht die „Kosten – Nutzenrechnung" für die Aufnahme und Verwendung dieser beiden biometrischer Daten in den sogenannten Hochsicherheitspässen in Österreich aus?

61. Worin liegt der entscheidende – zusätzliche - Sicherheitsgewinn durch die Einführung biometrischer Merkmale durch die Verwendung sogenannter Hochsicherheitspässe?

62. Welche Strafbestimmungen sind bei einer missbräuchlichen Verwendung von biometrischen Personendaten heranzuziehen?

63. Welche unabhängige Behörde hat in Österreich die Einhaltung datenschutzrechtlicher Bestimmungen bei elektronisch lesbaren Hochsicherheitspässen mit biometrischen Kennzeichen zu kontrollieren und Missbrauch zu verhindern?

64. Benötigt Österreich eine Novelle des Datenschutzgesetzes auch deshalb, weil zunehmend private Unternehmen biometrische Merkmale verlangen, verwenden und verarbeiten?