ARTIKEL-29-DATENSCHUTZGRUPPE

1710/05/DE-rev
WP 112
04/09/12

Stellungnahme 3/2005

zur Umsetzung der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten

(ABl. L 385 vom 29.12.2004, S. 1-6)

Angenommen am 30. September 2005

Inhaltsverzeichnis

Entwurf einer Stellungnahme zur Umsetzung der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABl. L 385 vom 29.12.2004, S. 1-6) 3

1. Einführung 3
1.1. Allgemeines 3
1.2. Geschichte und Hintergrund der Verordnung (EG) Nr. 2252/2004 des Rates 4
1.3. Frühere Stellungnahmen der Datenschutzgruppe 5
1.4. Resolution der Internationalen Konferenz der Datenschutzbeauftragten 7

2. Integration biometrischer Merkmale in Pässe, andere Reisedokumente und Identitätskarten 7
2.1. Allgemeine Betrachtungen 7
2.2. Ethische Risiken bei der Verwendung biometrischer Merkmale in Pässen, anderen Reisedokumenten und Identitätskarten 8
2.3. Gesetzgeberische Aspekte der Integration biometrischer Merkmale 9
a) Vorbehalte gegenüber einer zentralen Biometriedatenbank auf europäischer oder nationaler Ebene 9
b) Beschränkung des Zugangs zu biometrischen Daten auf die zuständigen Behörden 9
2.4. Technische Aspekte 10
a) Integration eines digitalisierten Gesichtsbilds 11
b) Integration zusätzlicher biometrischer Merkmale, insbesondere Fingerabdrücke 11

3. Schlussfolgerungen 12

Stellungnahme 3/2005
zur Umsetzung der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten
(ABl. L 385 vom 29.12.2004, S. 1-6)

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einführung

1.1. Allgemeines

In ihrem „**Arbeitspapier über Biometrie"[2]** hebt die Datenschutzgruppe Folgendes hervor: „Die rasanten Fortschritte auf dem Gebiet der biometrischen Verfahren und ihre in jüngster Zeit zunehmende Anwendung in unterschiedlichsten Bereichen machen eine sorgfältige Prüfung aus Datenschutzsicht erforderlich. Ein weit verbreiteter und unkontrollierter Einsatz der Biometrie bietet Anlass zu Sorge um den Schutz der Grundrechte und -freiheiten des Einzelnen. Biometrische Daten sind Daten besonderer Art, da sie sich auf die verhaltenstypischen und physiologischen Merkmale einer Person beziehen und unter Umständen ihre eindeutige Identifizierung ermöglichen."

Seit diesen grundlegenden Ausführungen zur Biometrie haben sich in der Gesetzgebung rasante Entwicklungen vollzogen. Der Europäische Rat (Thessaloniki, 19./20. Juni 2003) bekräftigte, dass in der Europäischen Union ein kohärenter Ansatz in Bezug auf biometrische Identifikatoren oder biometrische Daten für Dokumente für Drittstaatsangehörige, Pässe für EU-Bürger und Informationssysteme (VIS und SIS II) verfolgt werden muss. Im Herbst 2003 legte die Europäische Kommission einen Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung Nr. 1683/95 über eine einheitliche Visagestaltung sowie einen Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung Nr. 1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige vor.

---

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_de.htm.

[2] MARKT/10595/03/DE – WP 80, angenommen am 1. August 2003.

1.2. Geschichte und Hintergrund der Verordnung (EG) Nr. 2252/2004 des Rates

Am 18. Februar 2004 legte die Europäische Kommission einen Vorschlag für eine Verordnung über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger vor.[3] Der Vorschlag zielte darauf ab, die Sicherheit von Pässen zu erhöhen, indem ein verbindlicher Rechtsakt über Mindestnormen für harmonisierte Sicherheitsmerkmale geschaffen und zugleich durch die Einführung biometrischer Identifikatoren eine verlässliche Verbindung zwischen dem Inhaber und dem Dokument hergestellt wird. Damit würden die Mitgliedstaaten auch die Erfordernisse des „US Visa Waiver Program" in Übereinstimmung mit internationalen Normen erfüllen. In ihrem Vorschlag sprach sich die Kommission dafür aus, Pässe und andere Reisedokumente zwingend mit einem Datenträger auszustatten, der ein Gesichtsbild enthält. Den Mitgliedstaaten wurde die Möglichkeit eingeräumt, im Einklang mit ihren innerstaatlichen Rechtsvorschriften zusätzlich Fingerabdrücke in die Pässe aufzunehmen. Des Weiteren regte die Kommission an, den biometrischen Identifikator auf einem Datenträger mit ausreichender Kapazität zu speichern. Hierfür käme ein kontaktloser Chip in Frage, aber auch ein sonstiger Datenträger, der die erforderliche Kapazität aufweist; über die Einzelheiten sollten die technischen Sachverständigen im zuständigen Ausschuss entscheiden. Der Verordnungsvorschlag eröffnete auch die Möglichkeit, im Hinblick auf ein künftiges Europäisches Passregister Fingerabdrücke in einer nationalen Datenbank zu speichern.

Im Sommer 2004 befasste sich die Visa-Arbeitsgruppe mit dem Vorschlag. Am 6. Oktober 2004 wurde der Vorschlag abschließend im Strategischen Ausschuss für Einwanderungs-, Grenz- und Asylfragen (SCIFA) behandelt und an das Europäische Parlament weitergeleitet. In seiner endgültigen Fassung sah der Vorschlag das digitale Gesichtsbild als erstes – obligatorisches – biometrisches Merkmal und Fingerabdrücke als zweites – fakultatives – biometrisches Merkmal vor.

Im Anschluss an die Tagung des Rates „Justiz und Inneres" vom 25.-26. Oktober 2004 wurde der Vorschlag dahingehend geändert, dass beide biometrischen Merkmale zwingend vorgeschrieben wurden[4].

Die (nicht bindende) legislative Entschließung des Europäischen Parlaments zu dem Vorschlag der Kommission für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger vom 2. Dezember 2004[5] wurde mit 471 Jastimmen gegen 118 Neinstimmen und 6 Enthaltungen verabschiedet. Das Parlament befürwortete die Einführung von Pässen mit Gesichtsbild mit der Begründung, dass dieses biometrische Element Passfälschungen erschweren werde. Nach Auffassung des Parlaments werden die biometrischen Daten sicherstellen, dass es sich bei der Person, die einen Reisepass vorlegt, auch tatsächlich um die Person handelt, für die das Dokument ursprünglich ausgestellt wurde. Das Parlament wies darauf hin, dass bei der Integration der

---

[3] KOM(2004) 116 endg. (ABl. C 98 vom 23.4.2004, S. 39).

[4] Ratsdokument 15139/2004.

[5] Legislative Entschließung des Europäischen Parlaments zu dem Vorschlag der Kommission für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger (KOM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN&LEVEL=2&NAV=X.

biometrischen Elemente Persönlichkeits- und Datenschutzrechte nicht verletzt werden dürften, und lehnte daher die obligatorische Aufnahme von Fingerabdrücken und die Schaffung einer zentralen Datenbank der Pässe und Reisedokumente der Europäischen Union ab. Gemäß der legislativen Entschließung vom 2. Dezember 2004 sollten die biometrischen Daten in den Pässen nur verwendet werden, um die Echtheit des Dokuments und die Identität des Inhabers zu prüfen; außerdem sollten sie auf einem „Datenträger mit ausreichender Kapazität und einem hohen Sicherheitsstandard“ gespeichert werden, „der geeignet ist, die Integrität, Echtheit und Vertraulichkeit der gespeicherten Daten zu schützen“. Die Entschließung sah ferner vor, den Zugang zu den biometrischen Daten auf die für das Lesen, Speichern, Verändern und Löschen der Daten zuständigen Behörden der Mitgliedstaaten zu beschränken. Das Parlament nahm einen Änderungsvorschlag an, welcher ausdrücklich vorsah, dass „keine zentrale Datenbank der Pässe und Reisedokumente der Europäischen Union geschaffen [wird], die die biometrischen und sonstigen Daten aller Inhaber von EU-Pässen enthält“. Im Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) vom 25. Oktober 2004 heißt es: „Die Schaffung einer zentralen Datenbank würde gegen den Zweck und den Grundsatz der Verhältnismäßigkeit verstoßen. Überdies würde dies das Risiko des Missbrauchs und der Zweckentfremdung erhöhen. Schließlich würde dadurch auch die Gefahr größer, dass biometrische Identifikatoren als ‚Zugangsschlüssel’ zu verschiedenen Datenbanken verwendet werden, um so Datensätze miteinander zu verknüpfen.“

Der Rat nahm die Verordnung (EG) Nr. 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Reisedokumenten am 13. Dezember 2004 auf Grundlage der Vorlage des Rates „Justiz und Inneres“ vom 25.-26. Oktober 2004 an.[6] Die Ratsverordnung sieht die obligatorische Aufnahme des digitalen Gesichtsbilds als erstes biometrisches Merkmal und von Fingerabdrücken als zweites biometrisches Merkmal vor; den Anregungen und Änderungswünschen des Parlaments wurde vom Rat nicht Rechnung getragen. Die Verordnung ist gemäß ihrem Artikel 6 am 18. Januar 2005 in Kraft getreten. In diesem Artikel heißt es ferner: „Die Mitgliedstaaten wenden die Verordnung

a) in Bezug auf das Gesichtsbild spätestens 18 Monate,

b) in Bezug auf Fingerabdrücke spätestens 36 Monate

nach Erlass der in Artikel 2 genannten Maßnahmen an.“

Am 28. Februar 2005 nahm die Europäische Kommission ihre „Entscheidung über die technischen Spezifikationen zu Normen für Sicherheitsmerkmale und biometrischen Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisepässen”[7] an, die sich auf Artikel 2 der Verordnung (EG) Nr. 2252/2004 des Rates stützt.

1.3. Frühere Stellungnahmen der Datenschutzgruppe

Am 18. August 2004 richtete der Vorsitzende der Datenschutzgruppe ein Schreiben an den Präsidenten des Europäischen Parlaments, den Vorsitzenden des LIBE-Ausschusses, den Generalsekretär des Rates der Europäischen Union, den Präsidenten der Europäischen

---

6 ABl. L 285 vom 29.12.2004, S. 1-6.

7 C(2005) 409 endg.

Kommission, den Generaldirektor der GD Unternehmen und den Generaldirektor der GD Justiz und Inneres, das folgende konkrete Punkte enthielt:[8]

1. Die Datenschutzgruppe lehnt die Speicherung der biometrischen und sonstigen Daten aller Inhaber von EU-Pässen in einer zentralen Datenbank der Pässe und Reisedokumente der Europäischen Union entschieden ab.

2. Der Zweck der Aufnahme biometrischer Merkmale in Pässe und Reisedokumente muss in der Verordnung bestimmt werden, er muss eindeutig, angemessen, verhältnismäßig und klar sein.

3. Die Mitgliedstaaten gewährleisten durch solide technische Mittel, dass die Pässe ein Speichermedium mit ausreichender Kapazität enthalten, das geeignet ist, die Integrität, Echtheit und Vertraulichkeit der gespeicherten Daten zu schützen.

4. Die Verordnung bestimmt, welche Stellen zum Zugriff auf das Speichermedium berechtigt sind und zu welchen Zwecken (Lesen, Speichern, Verändern oder Löschen der Daten).

5. Die Mitgliedstaaten richten ein Register der zuständigen Behörden ein.

Der Vorsitzende wies in dem Schreiben darauf hin, dass die Sicherheitsmerkmale in Pässen und Reisedokumenten für die gesamte Gültigkeitsdauer des Dokuments gültig und gewährleistet sein müssten. Die ausstellenden Behörden seien für die Sicherheitsstandards und die erforderliche Infrastruktur zuständig. Etwaige diesbezügliche Mängel, die bei der Bearbeitung und Ausstellung des Dokuments oder während seiner Gültigkeitsdauer aufträten, könnten nicht den Bürgern angelastet werden.

Abschließend verwies er auf das Arbeitspapier über Biometrie (WP 80), das am 1. August 2003[9] von der Datenschutzgruppe angenommen wurde, und auf die Stellungnahme zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel (WP 96), angenommen am 11. August 2004[10].

In einem weiteren, an den Vorsitzenden des LIBE-Ausschusses und den Präsidenten des Rates der Europäischen Union gerichteten Schreiben vom 30. November 2004 sprach sich der Vorsitzende der Datenschutzgruppe gegen die Aufnahme eines zweiten obligatorischen biometrischen Merkmals aus. Er betonte, die Einführung eines weiteren biometrischen Merkmals lasse es umso dringlicher erscheinen, dass ein sicheres und zuverlässiges System eingesetzt werde, das die Wahrung des Grundrechts auf Privatsphäre gewährleiste.

Hierzu ist auch die Stellungnahme der Datenschutzgruppe vom 23. Juni 2005 (WP 110) zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für

---

8 Schreiben des Vorsitzenden der Artikel-29-Datenschutzgruppe an den Präsidenten des Europäischen Parlaments, den Vorsitzenden des LIBE-Ausschusses, den Generalsekretär des Rates der Europäischen Union, den Präsidenten der Europäischen Kommission, den Generaldirektor der GD Unternehmen und den Generaldirektor der GD Justiz und Inneres vom 18. August 2004 (nicht veröffentlicht).

9 MARKT/10595/03/DE – WP 80, angenommen am 1. August 2003.

10 MARKT/11224/03/DE – WP 96, angenommen am 11. August 2004.

einen kurzfristigen Aufenthalt (KOM(2004) 835 endg.)[11] zu berücksichtigen. Die Stellungnahme nimmt Bezug auf den im Arbeitspapier über Biometrie vertretenen Standpunkt und fordert angemessene Sicherheitsvorkehrungen für die Verarbeitung biometrischer Daten im VIS.

1.4. Resolution der Internationalen Konferenz der Datenschutzbeauftragten

Am 16. September 2005 hat die 27. Internationale Konferenz der Datenschutzbeauftragten in Montreux die **Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten** angenommen.[12] Unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte, fordert die Konferenz in ihrer Resolution

„1. wirksame Schutzmaßnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,

3. die technische Beschränkung der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage."

2. Integration biometrischer Merkmale in Pässe, andere Reisedokumente und Identitätskarten

Artikel 1 Absatz 2 der Verordnung (EG) Nr. 2252/2004 schreibt zwingend vor, dass die Pässe von EU-Bürgern Gesichtsbild und Fingerabdrücke als biometrische Merkmale enthalten. Gemäß Artikel 6 der Verordnung und im Einklang mit der Entscheidung der Europäischen Kommission K(2005) 409 haben die Mitgliedstaaten die Integration des digitalisierten Gesichtsbilds in ihre Pässe bis spätestens 28. August 2006 und die der Fingerabdrücke bis spätestens 28. Februar 2008 umzusetzen. Die ersten Mitgliedstaaten werden die so genannten ePässe, ausgestattet mit einem auf einem RFID-Chip gespeicherten digitalisierten Gesichtsbild, im Herbst 2005 einführen. In den Mitgliedstaaten, in denen Identitätskarten ausgestellt werden, gibt es Überlegungen, auch in diese Ausweise biometrische Merkmale zu integrieren.

2.1. Allgemeine Betrachtungen

Die Aufnahme biometrischer Merkmale in Pässe wird weit reichende Folgen für die Inhaber der Reisedokumente haben. Daher darf sie nicht ohne angemessene Bewertung der Auswirkungen auf die Persönlichkeitsrechte erfolgen. Bisher enthielten Pässe und andere Reisedokumente eine Beschreibung einiger biometrischer Merkmale in Form eines Lichtbilds und Angaben zu Geschlecht, Größe oder Augenfarbe. Nach Durchführung der Verordnung (EG) Nr. 2252/2004 des Rates müssen die Bürger Europas ihre biometrischen Daten in

[11] MARKT/1022/05/DE.

[12] http://www.privacyconference2005.org.

digitalisierter Form zur Verfügung stellen. Diese Daten können in Datenbanken gespeichert und für zahlreiche nicht vorhersehbare Zwecke verfügbar gemacht werden.

2.2. Ethische Risiken bei der Verwendung biometrischer Merkmale in Pässen, anderen Reisedokumenten und Identitätskarten

Die Verwendung biometrischer Merkmale in Pässen, anderen Reisedokumenten und Identitätskarten ist mit zahlreichen ethischen Risiken verbunden. Im Oktober 2004 ist das mit Gemeinschaftsmitteln des Sechsten Rahmenprogramms für Forschung und technologische Entwicklung (6. RP) finanzierte Projekt BITE (Biometric Identification Technology Ethics)[13] angelaufen, mit dem die Forschung zu Fragen der Bioethik im Kontext der Biometrie gefördert und eine öffentliche Debatte hierüber angestoßen werden soll. Im Juni 2006 wird hierzu eine öffentliche Konsultation durchgeführt. Ein weiteres Projekt, das von der EU im Rahmen des 6. RP gefördert wird, trägt die Bezeichnung FIDIS[14] (Future of Identity in the Information Society); es wird von einem Konsortium europäischer Hochschulen und Unternehmen sowie weiterer öffentlicher und privater Einrichtungen durchgeführt. Ziel des Projekts ist es, Anforderungen an das künftige Identitätsmanagement in der europäischen Informationsgesellschaft zu formulieren und einen Beitrag zu den benötigten Technologien und Infrastrukturen zu leisten.[15]

Gemäß einer im Auftrag des LIBE-Ausschusses des Europäischen Parlaments durchgeführten Prospektivstudie[16] sollten Ausweichverfahren als wesentliche Sicherheitsvorkehrungen für die Einführung biometrischer Systeme zur Verfügung stehen, da diese Systeme weder für jedermann geeignet noch vollkommen fehlerfrei sind. Durch Umsetzung und Einsatz dieser Verfahren soll die Würde von Menschen, die den Erfassungsvorgang nicht erfolgreich durchführen konnten, gewahrt und im Übrigen verhindert werden, dass Unzulänglichkeiten des Systems zu ihren Lasten gehen.[17]

Die Diskussion dreht sich u. a. um den Aspekt, dass staatliche Institutionen und andere öffentliche Behörden in der Lage sein werden, riesige Mengen an sensiblen Daten über die Bürger zu sammeln und zu speichern. In diesem Zusammenhang ist insbesondere darauf hinzuweisen, dass bei der Erfassung biometrischer Merkmale Daten vom *Körper* eines Menschen erhoben werden.

Ein weiterer Aspekt ist, dass biometrische Merkmale wie Fingerabdrücke bislang vor allem im Zusammenhang mit Straftaten erfasst wurden. Es stellt sich die Frage, ob die Bürger Europas bereit sind, ihre Fingerabdrücke auch für andere Zwecke zur Verfügung zu stellen.

Darüber hinaus gibt es weitere Bedenken unterschiedlicher Art: Personen, die ihre Identität u. U. nicht ohne weiteres nachweisen können, beispielsweise Migranten, könnten unter einem

---

[13] http://www.biteproject.org/

[14] http://www.fidis.net

[15] Zwei weitere aus Mitteln des 6. RP geförderte Projekte, BIOSEC und BIOSECURE, befassen sich ebenfalls bis zu einem gewissen Grad mit diesem Thema, siehe http://www.biosec.org und http://www.biosecure.info.

[16] „Biometrics at the frontiers: assessing the impact on Society“, Februar 2005 (Biometrie an den Grenzen: Abschätzung der Folgen für die Gesellschaft, Institute for Prospective Technological Studies, Gemeinsame Forschungsstelle, Europäische Kommission).

[17] „Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, Council of Europe“, 2005 (Fortschrittsbericht zur Anwendung der Grundsätze der Konvention des Europarates Nr. 108 auf die Erfassung und Verarbeitung biometrischer Daten), Seite 11.

solchen System zu Unrecht zur Zielscheibe werden, Menschen mit Behinderungen, die es ihnen nicht erlauben, sich den biometrischen Prüfungen zu unterziehen, könnten stigmatisiert werden, und sensible medizinische Daten könnten Unbefugten zugänglich werden. In der Praxis sind die datenschutzrechtlichen Vorschriften von Land zu Land unterschiedlich, was Auswirkungen auf die gemeinsame Nutzung von Daten und die Zusammenarbeit zwischen verschiedenen Datenbanken hat.

Bei der Speicherung von Fingerabdrücken ist insoweit Vorsicht geboten, als von Korrelationen zwischen bestimmten Papillarmustern und Krankheiten gesprochen wird. So sollen z. B. bestimmte Papillarmuster von der Ernährung der Mutter (und damit des Embryos) im dritten Schwangerschaftsmonat abhängen.[18] Auch bei Leukämie und Brustkrebs gibt es anscheinend einen statistischen Zusammenhang mit bestimmten Papillarmustern. Auch wenn direkte oder präzise Korrelationen für diese Fälle bisher nicht bekannt sind, ist hierüber doch eine wissenschaftliche Diskussion im Gange, die nicht ignoriert werden darf.

2.3. Gesetzgeberische Aspekte der Integration biometrischer Merkmale

a) Vorbehalte gegenüber einer zentralen Biometriedatenbank auf europäischer oder nationaler Ebene

In seiner legislativen Entschließung vom 2. Dezember 2004 fordert das Europäische Parlament, keine zentrale Datenbank der Pässe und Reisedokumente der Europäischen Union zu schaffen, die die biometrischen und sonstigen Daten aller Inhaber von EU-Pässen enthält. Die Datenschutzgruppe unterstützt diese Forderung und stellt fest, dass die Einwände, die gegen zentrale Datenbanken von Pässen und Reisedokumenten bzw. Identitätskarten auf nationaler Ebene vorgebracht werden, auch in Bezug auf eine zentrale europäische Datenbank der EU-Pässe und -Reisedokumente gelten.

Die Schaffung einer zentralen Datenbank, die personenbezogene Daten und insbesondere biometrische Daten aller Bürger (Europas) enthält, könnte gegen den Grundsatz der Verhältnismäßigkeit verstoßen. Eine zentrale Datenbank würde das Risiko des Missbrauchs und der widerrechtlichen Aneignung sowie der Zweckentfremdung erhöhen. Schließlich würde dadurch auch die Gefahr größer, dass biometrische Identifikatoren als „Zugangsschlüssel“ zu verschiedenen Datenbanken verwendet werden, um so Datensätze miteinander zu verknüpfen.

b) Beschränkung des Zugangs zu biometrischen Daten auf die zuständigen Behörden

Die in Pässen, anderen Reisedokumenten oder Identitätskarten enthaltenen biometrischen Merkmale sind hoch sensible Daten. Daher muss gewährleistet sein, dass die auf dem Chip gespeicherten Daten allein den zuständigen Behörden zugänglich sind. Ein unbefugter Zugang ist nicht hinnehmbar. Daher unterstützt die Datenschutzgruppe die Forderung des Europäischen Parlaments, dass jeder Mitgliedstaat ein Register der zuständigen Behörden und der ermächtigten Stellen gemäß Artikel 3 der Verordnung (EG) Nr. 2252/2004 führen sollte. Jeder Mitgliedstaat sollte dieses Register und gegebenenfalls dessen regelmäßige Aktualisierungen der Kommission übermitteln, die ein aktualisiertes elektronisches Register führt und jährlich eine Zusammenstellung der einzelstaatlichen Register veröffentlicht.

---

[18] FIDIS, „A study on PKI and biometrics“ (Studie zu PKI und Biometrie), S. 68.

Im Falle einer Zurückweisung bei der Grenzkontrolle oder bei anderen Kontrollen durch die zuständigen Behörden müssen die betroffenen Personen über die Gründe für die Zurückweisung unterrichtet werden, über ihre Möglichkeiten, ihren Standpunkt darzulegen, sowie über die zuständigen Stellen, bei denen sie Einspruch erheben können.

2.4. Technische Aspekte

Es gibt technische Risiken unterschiedlicher Art; sie betreffen die Integration des kontaktlosen Chips (RFID-Chips) und der auf ihm gespeicherten biometrischen Merkmale.

In seiner legislativen Entschließung vom 2. Dezember 2004 fordert das Europäische Parlament, dass der Pass „einen Datenträger mit ausreichender Kapazität und einem hohen Sicherheitsstandard" enthalten muss, „der geeignet ist, die Integrität, Echtheit und Vertraulichkeit der gespeicherten Daten zu schützen". Die Datenschutzgruppe hat diese Forderung unterstützt[19], ihr wurde jedoch vom Rat nicht Rechnung getragen. Der von der Verordnung (EG) Nr. 2252/2004 vorgesehene RFID-Chip, der ISO-Norm 14443 entspricht, birgt zahlreiche Risiken für das Recht der europäischen Bürger auf Privatsphäre. Die Entscheidung der Kommission vom 28. Februar 2005[20] ist nicht geeignet, die Rechte der Bürger zu wahren, da die Kommunikation zwischen dem RFID-Chip und dem Lesegerät abgehört und die Daten von Unbefugten ausgelesen werden können.

Die Risiken, die sich aus der Integration von RFID-Chips in Pässe, andere Reisedokumente oder Identitätskarten ergeben, ebenso wie diejenigen, die durch die Speicherung biometrischer Merkmale auf den Chips entstehen, machen eine Sicherheitsarchitektur erforderlich, die darauf ausgerichtet ist, ein höheres Maß an Vertraulichkeit der auszutauschenden Daten zu gewährleisten. Die Datenschutzgruppe ist sich der inhärenten Probleme bewusst und hält daher eine globale PKI (Public Key Infrastructure) für erforderlich. Die Zertifikate für öffentliche Schlüssel (public keys) enthalten Informationen über den Inhaber. Jedes digitale Zertifikat lässt sich eindeutig zu der Person zurückverfolgen, der es ausgestellt wurde. Digitale Zertifikate sind so unverwechselbar wie Sozialversicherungsnummern, Kreditkartennummern oder Krankenversicherungsnummern. Sie können allerdings missbraucht werden, um einem Zertifikatsinhaber den Zugang zu Dienstleistungen zu verweigern. Außerdem können transaktionsgenerierte Daten, die mit Zertifikaten übertragen werden, mit Überwachungswerkzeugen herausgefiltert und auf elektronischem Wege an Dritte, die Polizei oder andere Behörden weitergegeben werden.

Zum Schutz gegen diese Risiken muss ein Schutzprofil (Protection Profile, PP) geschaffen werden, das den „Common Criteria for Information Technology Security Evaluation (Common Criteria – CC) vers. 2.1" (ISO-Norm 15408) entspricht. Diese „gemeinsamen Kriterien" bieten eine allgemein anerkannte Lösung für IT-Sicherheitsprobleme. Ein Schutzprofil beschreibt ein IT-Sicherheitskonzept, das vollständig, konsistent und kohärent sein muss. Das Schutzprofil sollte von dem Ausschuss erstellt werden, auf den Artikel 5 der Verordnung (EG) Nr. 2252/2004 Bezug nimmt. Im Einklang mit den vom Europäischen Parlament in seiner legislativen Entschließung vom 2. Dezember 2004 unterbreiteten

---

[19] Schreiben des Vorsitzenden der Artikel-29-Datenschutzgruppe an den Präsidenten des Europäischen Parlaments, den Vorsitzenden des LIBE-Ausschusses, den Generalsekretär des Rates der Europäischen Union, den Präsidenten der Europäischen Kommission, den Generaldirektor der GD Unternehmen und den Generaldirektor der GD Justiz und Inneres vom 18. August 2004 (nicht veröffentlicht).

[20] C(2005) 409 endg.

Änderungsanträgen schlägt die Datenschutzgruppe vor, dass der Ausschuss von Sachverständigen unterstützt wird, die von ihr benannt werden.

a) Integration eines digitalisierten Gesichtsbilds

Im Einklang mit der Entscheidung der Europäischen Kommission vom 28. Februar 2005 haben die Mitgliedstaaten die Integration des digitalisierten Gesichtsbilds in ihre Pässe bis spätestens 28. August 2006 umzusetzen. Gemäß Artikel 1 der Entscheidung und Ziffer 5.2 des Anhangs zur Entscheidung müssen die Mitgliedstaaten die Daten auf dem Chip durch ein Sicherheitsmerkmal schützen, das als einfache Zugangskontrolle oder einfacher Zugriffsschutz (Basic Access Control, BAC) bezeichnet wird. BAC wird von der Internationalen Zivilluftfahrt-Organisation (International Civil Aviation Organisation, ICAO) empfohlen, ist jedoch nicht zwingend vorgeschrieben[21]. Der BAC-Mechanismus soll unautorisiertes Auslesen der Daten (Skimming) sowie unautorisiertes Abhören der Kommunikation (Eavesdropping) verhindern. Er soll gewährleisten, dass der Zugriff auf die Daten und insbesondere auf die biometrischen Daten nur dann möglich ist, wenn vor dem Auslesen der Daten vom Chip ein optischer Kontakt zwischen Pass und Lesegerät hergestellt wird, um aus den Feldern der maschinenlesbaren Zone (Machine Readable Zone, MRZ) des Passes einen dokumentspezifischen einfachen Zugriffsschlüssel (Document Basic Access Key) zu bilden. Der Zugriffsschlüssel wird aus der Passnummer, dem Geburtsdatum und dem Ablaufdatum des Passes berechnet. Erst wenn dieser Zugriffsschlüssel gebildet ist, kann das Lesegerät die auf dem RFID-Chip gespeicherten Daten auslesen. Aus Sicherheitsgründen werden die Daten verschlüsselt übertragen. Hierzu ist ein zertifizierter Sicherheitschip mit kryptografischem Koprozessor erforderlich. [22]

BAC stellt jedoch kein angemessenes Sicherheitsmerkmal dar. Die einfache Zugangskontrolle erfolgt auf Grundlage der maschinenlesbaren Zone (MRZ) des Passes, deren Daten nicht streng vertraulich behandelt werden. Wenn ein EU-Bürger z. B. eine Karte für ein Großereignis wie die Fußball-Weltmeisterschaft 2006 in Deutschland oder die Fußball-Europameisterschaft 2008 in Österreich und der Schweiz kaufen möchte, muss er seinen Namen, sein Geburtsdatum, die Nummer seines Reisepasses oder Personalausweises sowie das Ausstellungsdatum des Dokuments in ein Internetformular eintragen. Dieses Verfahren wurde bereits für die Fußball-Europameisterschaft 2004 in Portugal eingesetzt und wird künftig auch für andere Veranstaltungen wie Konzerte oder Sportereignisse wie die Olympischen Spiele oder die Leichtathletik-Weltmeisterschaften genutzt werden. Da Privatunternehmen in manchen Mitgliedstaaten Reisepässe oder Personalausweise als Sicherheit für offene Forderungen kopieren, sind die Bestandteile des Document Basic Access Key nicht geheim und es ist zu befürchten, dass der für die einfache Zugangskontrolle verwendete Algorithmus irgendwann im Internet verfügbar sein wird.

b) Integration zusätzlicher biometrischer Merkmale, insbesondere Fingerabdrücke

Die Umstände, unter denen Fingerabdrücke erfasst werden, müssen absolute Verlässlichkeit gewährleisten. Während die ICAO ein digitalisiertes Gesichtsbild nicht als sensibel einstuft,

---

[21] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1 (Technischer Bericht der ICAO über PKI für maschinenlesbare Reisedokumente mit ICC-Lesezugriff), veröffentlicht am 1. Oktober 2004, S. 16.

[22] Die so genannte Essen Group hat für die sichere Übertragung eine eigene Software unter der Bezeichnung „Golden Reader Tool" entwickelt. Der „Essen Group" gehören öffentliche Behörden, IT-Sicherheitsunternehmen sowie Hersteller von Reisedokumenten aus Deutschland, den Niederlanden und dem Vereinigten Königreich an.

da der Pass weiterhin ein Lichtbild des Inhabers enthält, erkennt sie an, dass die Aufnahme von Fingerabdrücken und anderen zusätzlichen biometrischen Merkmalen in den Pass als hoch sensibel zu betrachten ist. Daher empfiehlt die ICAO einen als Extended Access Control bezeichneten speziellen Sicherheitsmechanismus[23]. Diese zusätzliche Zugangskontrolle funktioniert ähnlich wie die oben beschriebene einfache Zugangskontrolle BAC. Allerdings wird für Extended Access Control statt des Document Basic Access Key ein dokumentspezifisches erweitertes Zugriffsschlüsselpaar (Document Extended Access Key) verwendet. Für die Festlegung des (chipspezifischen) Document Extended Access Key ist der jeweilige Staat zuständig. Dieses Zugriffsschlüsselpaar besteht entweder aus symmetrischen Schlüsseln, die z. B. aus der MRZ oder einem „nationalen Hauptschlüssel" abgeleitet werden, oder einem asymmetrischen Schlüsselpaar mit zugehörigem Kartenzertifikat. Zahlreiche Einzelheiten dieser Sicherheitsmechanismen sind jedoch noch unklar.

Extended Access Control stellt einen Fortschritt bei den Sicherheitsvorkehrungen dar, ist jedoch ebenso wie Basic Access Control ein fakultativer Sicherheitsmechanismus[24]. Außerdem ist strittig, ob diese zusätzliche Zugangskontrolle von Nicht-Mitgliedstaaten umgesetzt wird. Die Europäische Kommission und die Mitgliedstaaten müssen gewährleisten, dass Reisepässe von EU-Bürgern, die Fingerabdruck-Daten enthalten, nicht von Lesegeräten gelesen werden können, die Extended Access Control nicht unterstützen.

3. Schlussfolgerungen

Die Aufnahme biometrischer Merkmale in Pässe, andere Reisedokumente und Identitätskarten wirft zahlreiche ethische, rechtliche und technische Fragen auf. Daher weist die Datenschutzgruppe auf folgende Aspekte hin:

1. Der Einführung biometrischer Merkmale in Pässen, anderen Reisedokumenten oder Identitätskarten muss eine umfassende Debatte in der Gesellschaft vorausgehen. Hierfür müssen die Ergebnisse des BITE-Projekts abgewartet werden.

2. Um die der Biometrie inhärenten Risiken zu vermindern, müssen zu einem möglichst frühen Zeitpunkt wirksame Schutzmaßnahmen durchgeführt werden. Zu diesem Zweck muss der Ausschuss, auf den Artikel 5 der Verordnung (EG) Nr. 2252/2004 Bezug nimmt, unterstützt durch von der Datenschutzgruppe benannte Sachverständige, ein Schutzprofil erstellen.

3. Die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, deren Erfassung und Speicherung mit Einwilligung der betroffenen Person zu Vertragszwecken erfolgt, muss gewährleistet sein.

4. Die Verwendung biometrischer Daten in Pässen und Identitätskarten muss mit technischen Mitteln auf den Zweck der Identitätsprüfung (Verifikation) durch Vergleich der

---

[23] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1 (Technischer Bericht der ICAO über PKI für maschinenlesbare Reisedokumente mit ICC-Lesezugriff), veröffentlicht am 1. Oktober 2004, S. 17.

[24] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1 (Technischer Bericht der ICAO über PKI für maschinenlesbare Reisedokumente mit ICC-Lesezugriff), veröffentlicht am 1. Oktober 2004, S. 17, 21 und 22.

Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage beschränkt werden.

5. Die Europäische Kommission und die Mitgliedstaaten müssen gewährleisten, dass Reisepässe von EU-Bürgern, die Fingerabdruck-Daten enthalten, nicht von Lesegeräten gelesen werden können, die Extended Access Control nicht unterstützen.

6. Es muss gewährleistet sein, dass die auf dem Chip gespeicherten Daten allein den zuständigen Behörden zugänglich sind. Die Mitgliedstaaten richten ein Register der zuständigen Behörden ein.

Brüssel, den 30. September 2005

Für die Datenschutzgruppe
Der Vorsitzende
Peter Schaar