

## **Einführung eines elektronischen Passes (ePass) mit biometrischen Merkmalen**

(Beitrag des TLfD im Thüringer Landtagskurier Ausgabe 2/2005)

Bereits mit Artikel 7 des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 ist eine Änderung des § 4 Abs. 3 Passgesetz erfolgt, wonach in den Pass neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden dürfen. Die Arten der Merkmale sowie die technischen Einzelheiten hierzu wurden einem gesonderten Bundesgesetz vorbehalten.

### **Europarechtlich verbindliche Vorgaben**

Diese Befugnis hat zwischenzeitlich die Europäische Union an sich gezogen und mit der am 18. Januar 2005 in Kraft getretenen „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. EU Nr. L 385 S. 1) die Aufnahme biometrischer Merkmale in die Reisepässe der Unionsbürger verbindlich geregelt. Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß Artikel 249 des Vertrages zur Gründung der Europäischen Gemeinschaft unmittelbar in allen Mitgliedstaaten. Art. 1 Abs. 2 Satz 1 EG-PassVO sieht vor, dass die Pässe und Reisedokumente mit einem Speichermedium zu versehen sind, das ein Gesichtsbild enthält. Die Mitgliedstaaten haben nach Art. 1 Abs. 2 Satz 2 EG-PassVO auch Fingerabdrücke in interoperablen Formaten hinzu zu fügen. Schließlich ist in Art. 1 Abs. 2 Satz 3 EG-PassVO vorgesehen, dass die Daten zu sichern sind und das Speichermedium eine ausreichende Kapazität aufweisen und geeignet sein muss, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen. Mit der Festlegung der weiteren technischen Spezifikationen wurde nach Art. 2 EG-PassVO die Kommission in Form von Durchführungsbestimmungen im sog. „Komitologieverfahren“ ermächtigt. Die Kommission hat in ihrer „Entscheidung über die technischen Spezifikationen zu Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“ vom 28. Februar 2005 [K(2005) 409 endg] u. a. verbindliche Vorgaben zu den technischen Anforderungen an die im Pass gespeicherten biometrischen Merkmale sowie zu den Vorkehrungen zum Schutz dieser Daten vor Verfälschung und unbefugtem Zugriff gemacht, die ihrerseits größtenteils auf technische Standards und Normen u. a. der Internationalen Zivilluftfahrtorganisation (ICAO) der Vereinten Nationen verweisen. Mit dem Erlass dieser Durchführungsbestimmungen beginnen die Fristen des Art. 6 EG-PassVO zu laufen, die eine Anwendung der Verordnung in Bezug auf das

Gesichtsbild spätestens nach 18 Monaten (also am 1. September 2006) sowie in Bezug auf Fingerabdrücke nach 36 Monaten (also am 1. März 2008) vorschreiben.

### **Anwendung der EG-PassVO in Deutschland**

Wegen der unmittelbaren Geltung der Regelungen der EG-PassVO sind in den Mitgliedstaaten grundsätzlich keine Änderungen der nationalen Gesetze erforderlich. Der Bundesminister des Innern hat kürzlich angekündigt, mit der Ausgabe von Pässen, die den Anforderungen der EG-PassVO entsprechen zum 1. November 2005 zu beginnen. Dazu hat das Bundesministerium des Innern den Entwurf einer Zweiten Verordnung zur Änderung passrechtlicher Vorschriften (BR-Drs. 510/05) dem Bundesrat zur Zustimmung vorgelegt, mit dem die Passmusterverordnung, die Verordnung zur Durchführung des Passgesetzes und die Passgebührenverordnung den Vorgaben der EG-PassVO angepasst werden sollen. In letzterer soll u. a. die Gebühr für die Ausstellung eines ePasses von bislang 26 € auf 59 € erhöht werden. Die neuen ePässe sollen mit einem RFID-Chip ausgestellt werden, auf dem das Gesichtsbild sowie die anderen bereits jetzt aus dem Pass maschinenlesbaren Daten (Name, Vorname, Geburtstag, Geschlecht, Seriennummer und Gültigkeitsdauer) elektronisch gespeichert werden. Die Unverfälschtheit und Richtigkeit der im ePass gespeicherten Daten soll durch eine digitale Signatur sichergestellt werden. Der Schutz vor unbefugtem Zugriff, der bei einem kontaktlosen RFID-Chip durch Abhören der Funkkommunikation zwischen dem Pass und dem Lesegerät möglich ist, soll durch ein Zugriffskontrollsystem (Basic Access Control) realisiert werden, das durch das optische Einlesen der maschinenlesbaren Datenzone des Passes aktiviert wird und die Kommunikation mit dem Lesegerät kryptographisch verschlüsselt (Sitzungsschlüssel). Für die ab 2007 vorgesehene zusätzlich aufzunehmenden Fingerabdrücke ist wegen der Sensibilität der Daten vom Bundesministerium des Innern ein erweitertes Zugriffskontrollsystem (Extendend Access Control) vorgesehen, bei dem durch ein zusätzliches kryptographisches Protokoll der Zugriff nur von dafür speziell autorisierten Lesesystemen erfolgen kann.

### **Datenschutzrechtliche Fragen**

Mit dem ePass soll die eindeutige Identifizierung aller Passinhaber durch biometrische Merkmale ermöglicht werden. Dies kann einerseits einen Sicherheitsgewinn bei der Vorbeugung und Bekämpfung von Verbrechen ermöglichen. Damit verbunden sind aber auch Risiken für die Persönlichkeitsrechte der Passinhaber, die insbesondere darin zu sehen sind, dass diese Identifizierungsdaten neben dem Zweck der eindeutigen Identifizierung des Passinhabers durchaus geeignet sind, als Schlüssel zur Verknüpfung von Daten des Betroffenen aus den unterschiedlichsten Verwendungszusammenhängen zu dienen und damit umfassende Persönlichkeits- und Bewegungsprofile zu erstellen. Dies auch gerade deshalb, weil

die vorgesehenen biometrischen Merkmale durchaus auch von Dritten ohne Kenntnis des Betroffenen erhoben werden könnten (z. B. Fingerabdrücke an Gegenständen). Aus diesem Grund bedarf es aus datenschutzrechtlicher Sicht einer strengen Zweckbindung der im Pass gespeicherten personenbezogenen Daten sowie eines Schutzes gegen unbefugtes Auslesen dieser Daten aus dem Pass. In einer Entschließung der Datenschutzkonferenz des Bundes und der Länder vom 8. März 2002 wurde in diesem Zusammenhang gefordert, dass die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt bleiben soll, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber übereinstimmen. Eine Verwendung der Daten für andere öffentliche oder private Zwecke sollte ausgeschlossen werden und insbesondere keine Einrichtung zentraler Dateien erfolgen. Hierauf hat im Rahmen des EU-Rechtsetzungsverfahrens der Bundesbeauftragte für den Datenschutz in seiner Funktion als Vorsitzender der Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie in gleich lautenden Schreiben an das Europäische Parlament, den Rat und die Kommission hingewiesen. Mit Unterstützung des Europäischen Parlaments wurde daraufhin durch das zuständige Ratsgremium der ursprüngliche Kommissionsvorschlag um eine strenge Zweckbindungsregel in Art. 4 Abs. 3 EG-PassVO ergänzt sowie die Anforderung an das Speichermedium in Art. 1 Abs. 2 EG-PassVO aufgenommen, Integrität, Authentizität und Vertraulichkeit der Daten sicherzustellen und die Vorgabe für die technischen Spezifikationen nach Art. 2 Buchstabe b EG-PassVO formuliert, einen unbefugten Zugriff auf die Daten im Pass zu verhindern. Die Zweckbindungsregel in Art. 4 Abs. 3 EG-PassVO, bestimmt eindeutig, dass die Daten des ePasses ausschließlich zur Identitätskontrolle vor Ort durch Vergleich der Merkmale des Passinhabers mit den auf dem Pass gespeicherten Daten ohne Rückgriff auf zentrale Datenbanken verwendet werden dürfen. Dies entspricht der geltenden Rechtslage des deutschen Passgesetzes. Bundesminister Schily hat bei der Vorstellung des ePasses am 1. Juni 2005 hierzu ausdrücklich erklärt, dass eine zentrale Speicherung der Passdaten nicht geplant sei. Damit erscheinen die derzeitigen Regelungen zur Zweckbindung der Passdaten vom Ansatz her ausreichend. Nicht abschließend beurteilt werden kann derzeit die Frage, ob mit der vorgesehenen technischen Lösung die Vorgaben der EG-PassVO zur Sicherstellung von Integrität, Authentizität und der Vertraulichkeit der auf dem Chip gespeicherten Daten durch entsprechende rechtliche, organisatorische und technische Maßnahmen erfüllt werden. Daher hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 1. Juni 2005 davor gewarnt, ohne die Festlegung von technischen und organisatorischen Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung auf der Grundlage eines umfassendes Datenschutz- und IT-Sicherheitskonzeptes bereits in diesem Jahr mit der Ausgabe der ePässe zu beginnen. Denn eine europarechtliche Verpflichtung hierzu besteht erst ab Mitte nächsten Jahres. Auch der Europäische Datenschutz-

beauftragte hat Anfang Juni 2005 auf Anfrage des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments u. a. darauf hingewiesen, dass eine Datensicherheitsanalyse des Verfahrens gerade deshalb erschwert wird, weil ein großer Teil der technischen Standards, auf die die Durchführungsbestimmungen der Kommission verweisen noch in der Entwicklung sind. Es bleibt daher zu hoffen, dass vor der Ausgabe der ePässe diese Fragen durch den Bund gelöst werden und es nicht am Ende der Entwicklung statt mehr weniger Sicherheit für die Bürger gibt.