

REPUBLIK ÖSTERREICH
D A T E N S C H U T Z R A T

A-1010 Wien, Ballhausplatz 2
Tel. ++43-1-531 15/2527
Fax: ++43-1-531 15/2702
e-mail: dsrpost@bka.gv.at
DVR: 0000019

GZ BKA-817.336/002-DSR/2008

An das
Bundesministerium für Inneres

Per Mail: bmi-III-3@bmi.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem das Passgesetz 1992, das
Gebührengesetz 1957 und das Konsulargebührengesetz 1992 geändert werden
Stellungnahme des Datenschutzrates

Der Datenschutzrat hat in seiner 182. Sitzung am 23.Juni 2008 mit einstimmig
beschlossen, zu der im Betreff genannten Novelle folgende Stellungnahme
abzugeben:

Aus Datenschutzperspektive wesentlicher Inhalt der Novelle ist zunächst der
Umstand, dass zufolge der Änderungen des PassG anlässlich der Pass-
Beantragung den Antragstellern zwei Fingerabdrücke („Papillarlinienabdrücke zweier
Finger“) abgenommen werden. Dies erfolgt primär dazu, Bilder dieser
Fingerabdrücke auf einem Datenträger im Pass zu speichern, um die
Fälschungssicherheit zu erhöhen bzw. einen automatisierten Abgleich zwischen
Passinhaber und Pass bewerkstelligen zu können.

Für die Erreichung der genannten Zwecke (Fälschungssicherheit, automatisierter
Abgleich) würden die bereits bis dato erfassten Lichtbilder ausreichen. Da die
Passmerkmale trotz Datenschutzbedenken jedoch auf EU-Ebene in
Verordnungsform (EG) Nr. 2252/2004 vorgegeben wurden, besteht national kein
Spielraum in der Frage der zu erhebenden Merkmale.

Der Datenschutzrat äußert aus gegebenem Anlass erneut den Wunsch, bei datenschutzrechtlich relevanten EU-Vorhaben rechtzeitig in die Verhandlungen eingebunden zu werden.

Durch die derzeitige Fassung des Gesetzesentwurfs in Zusammenschau mit dem unverändert bleibenden geltenden Text des § 22a PassG iVm § 3 Abs. 6 leg. cit. würde eine 4-monatige Speicherung der nunmehr bei der Antragstellung zur Einbringung in das Passdokument abgenommenen Fingerabdrücke sowohl bei der örtlich zuständigen Passbehörde als auch beim technischen Dienstleister ermöglicht. Es stellt sich die Frage nach der sachlichen Rechtfertigung für diese Frist. Die Behörde benötigt die Fingerabdrucksdaten zur Weiterleitung an den Dienstleister zur Einbringung in den Datenträger. Mit der gelungenen Übermittlung an diesen könnte daher eine sofortige Löschung Platz greifen. Auch der Dienstleister selbst scheint über den Zeitpunkt der technischen Einbringung der Daten in den Pass die Fingerabdrucksdaten nicht zu benötigen. Die Erläuterungen verweisen zur Begründung der 4-Monatsfrist auf nicht näher spezifizierte und daher zunächst nicht nachvollziehbare Reklamationsfälle. Wie der Datenschutzrat feststellen musste, handelt es sich bei der 4- Monatsfrist um eine eher willkürlich festgesetzte Frist. Es wird daher vorgeschlagen, diese auf das verwaltungstechnisch absolut notwendige Ausmaß zu reduzieren.

Die lokale Speicherung bei der Passbehörde stellt aufgrund technischer Gegebenheiten (Dienstleisterfunktion des Bundesministeriums für Inneres) de facto eine zentrale Speicherung dar.

Eine derartige Speicherung ist auch durch die obzitierte Verordnung (EG) Nr. 2252/2004 nicht geboten. Weiters ist anzumerken, dass nach der Rechtsprechung von VfGH und VwGH der Zweck der Dokumentation von Amtshandlungen nicht stets eine Datenspeicherung gebietet, sondern vielmehr dennoch eine Interessenabwägung vorzunehmen ist (vgl. VfGH E 7.3.2007, B 3517/05 oder VwGH E 19.12.2005, Zl. 2005/06/0140).

Hingewiesen sei als Vergleichsmaßstab schließlich noch auf die deutsche Rechtslage: Nach § 16 Abs. 2 letzter Satz des deutschen Passgesetzes sind die bei der Passbehörde gespeicherten Fingerabdrücke spätestens nach Aushändigung des Passes an den Passbewerber zu löschen. Eine derartige ausdrückliche Anordnung

erschiene auch für Österreich aus datenschutzrechtlicher und -politischer Sicht, auch im Lichte der gegebenen Rechtslage, diskussionswürdig.

Unterstrichen werden die Bedenken gegen eine mehrmonatige Speicherung durch die in § 22d Abs 1 PassG neu vorgesehene Ermächtigung des BMI, den Passbehörden, den Grenzkontrollbehörden und den Sicherheitsbehörden zur Wahrnehmung von Aufgaben der Kriminal- und Sicherheitspolizei das Auslesen der auf den Datenträgern in den Reisepässen gespeicherten Papillarlinienabdrücke durch die Zurverfügungstellung entsprechender Zertifikate zu ermöglichen.

Diese Vorgangsweise ist an dem Gebot der Zweckbindung („Reisedokumentenausstellung und –verwaltung sowie Vermeidung von Fälschungen“) zu messen, wie es an sich in § 22a Abs. 3 PassG normiert ist. Danach dürfen verarbeitete Papillarlinienabdrücke ausschließlich für die Identifizierung des Passinhabers und die Prüfung der Authentizität des Dokuments in Vollziehung dieses Gesetzes verwendet werden. Diese scheinbar strenge Zweckbindung wird mit § 22d Abs 1 PassG offenbar unterlaufen.

Auch die vorgesehene Überlassung von Zertifikaten zwecks Zugriff auf die Fingerabdrucksdaten an Behörden der Mitgliedstaaten der Europäischen Union gemäß § 22d Abs 1 ist problematisch zu sehen, da auf unbestimmte Regelungen auf Gemeinschaftsebene verwiesen wird.

Noch gravierendere Probleme wirft die Überlassung solcher Zertifikate an EU-Drittstaaten auf. In der Einräumung eines Zugriffs ist nämlich eine Übermittlung iSd § 4 Z 12 DSG zu sehen. Die Ermächtigung in § 22d Abs 2 PassG stellt zwar formal eine für EU-Drittstaatsübermittlungen erforderliche gesetzesrangige Norm iSd § 12 Abs 3 Z 3 DSG 2000 dar, die vom Empfangsstaat gewisse Anforderungen verlangt. Sie trifft aber keine Aussagen, in welcher rechtlichen Qualität sich ein Drittstaat den „innergemeinschaftlichen Rahmenbedingungen vergleichbaren Regelungen“ zu unterwerfen hat. Eine Zusage solcher Staaten zur Einhaltung eines bestimmten Datenschutzniveaus etwa in einer Form eines bloßen Ressortabkommens, würde es dem Innenministerium und Außenministerium ermöglichen, ohne parlamentarische Kontrolle Entscheidungen mit erheblicher Grundrechtsrelevanz und Datensicherheitsrelevanz zu treffen. Angesichts der Sicherheitsrisiken für die Betroffenen einerseits und dem fehlenden Mehrwert für die Republik Österreich andererseits erschiene es überlegenswert, auf eine Weitergabe der Zertifikate für

den Zugriff auf die Fingerabdrucksdaten an EU-Drittstaaten gänzlich zu verzichten bzw. diese nur unter der Voraussetzung zur Verfügung zu stellen, wenn ein angemessenes Datenschutzniveau in diesen Drittstaaten besteht.

Schließlich ist zu vermerken, dass eine Regelungslücke insofern besteht, als Bürgermeister außerhalb eines Sprengels einer Bundespolizeidirektion nicht als Passbehörden iSd § 16 PassG gelten, aber von der Bezirksverwaltungsbehörde ermächtigt werden können, Anträge entgegen zu nehmen (§ 16 Abs. 3 leg. cit.). Die in § 3 Abs 8 leg. cit. getroffene Dienstleisterregelung betreffend Datenerfassung greift insofern nicht ein und es erhebt sich die Frage, wie die Bürgermeister eine sichere Handhabung insbesondere der Fingerabdrucksdaten gewährleisten sollen.

Insgesamt empfiehlt der Datenschutzrat daher,

1. im PassG ausdrücklich die physische Löschung sämtlicher, bei der Passbeantragung bzw. -ausstellung anfallenden Fingerabdrucksdaten, die auf Datenträgern außerhalb des Passes gespeichert sind, sei es bei der Behörde, sei es bei einem technischen Dienstleister, sobald als möglich vorzusehen;
2. im PassG einen Zugriff auf die Fingerabdrucksdaten im Pass strikt auf den Zweck der Prüfung der Übereinstimmung der Identität von Passinhaber und der Person, auf die der Pass ausgestellt wurde, zu beschränken und eine sicherheitspolizeiliche bzw kriminalpolizeiliche Nutzung (zur Bekämpfung der Alltagskriminalität) auszuschließen; sowie
3. direkt im Passgesetz vorzusehen, dass ein Zugriff und eine Nutzung durch andere als EU-Staaten restriktiv geregelt wird und Leseberechtigungszeugnisse nur unter der Voraussetzung zur Verfügung gestellt werden dürfen, wenn ein angemessenes Datenschutzniveau in diesen Drittstaaten besteht;
4. gesetzliche Vorkehrungen zu treffen, die gewährleisten, dass die von den Bezirksverwaltungsbehörden zur Antragsentgegennahme ermächtigten Bürgermeister bei der Datenerhebung und Weiterleitung denselben Sicherheitsstandard einhalten, wie die Passbehörden selbst;

5. der Bundesregierung, alles zu unternehmen, damit auf europäischer Ebene weder eine verpflichtende Einrichtung zentraler nationaler Fingerabdrucksdateien betreffend Reisepassinhaber noch eine allfällige europäische Datei solchen Inhalts vorgesehen wird.

Abschließend regt der Datenschutzrat zu § 19 Abs. 3 des Entwurfes im Hinblick auf eine mögliche Diskriminierung der Minderjährigen an, auf die vorgesehene farbliche Unterscheidung der Personalausweise zu verzichten.

26. Juni 2008
Für den Datenschutzrat:
Der Vorsitzende:
WÖGERBAUER

Elektronisch gefertigt