

**Regierungsrat**

Rathaus / Barfüssergasse 24  
4509 Solothurn  
www.so.ch

Bundesamt für Polizei  
3003 Bern

20. September 2005

**Vernehmlassung zum Vorentwurf zur Änderung des Gesetzes und der Verordnung über die Ausweise für Schweizer Staatsangehörige**

Sehr geehrte Damen und Herren

Mit Schreiben vom 15. Juli 2005 hat uns das Eidgenössische Justiz- und Polizeidepartement zur Vernehmlassung zum Vorentwurf zur Änderung des Gesetzes und der Verordnung über die Ausweise für Schweizer Staatsangehörige (im Folgenden „VE AwG“ und „VE VAWG“ bezeichnet) eingeladen. Wir danken für die Möglichkeit zur Stellungnahme und äussern uns zu diesem Geschäft wie folgt:

**1. Allgemeine Vorbemerkungen**

Bereits der alte Pass (Modell 85) sowie der aktuelle maschinenlesbare Pass (Modell 2003) enthalten mit Gesichtsbild, Grösse und Unterschrift der Person grundsätzlich biometrische Daten.

Die Neuerung, welche die aktuelle Technologie ermöglicht, besteht darin, dass weitere und detailliertere Daten aufgenommen werden und diese – im Rahmen des Pilotprojektes vorerst das Gesichtsbild und evtl. Fingerabdrücke – auf einem Chip abgespeichert werden. Weil die Daten im künftigen biometrischen Pass elektronisch gespeichert sind, können diese automatisch mit den Daten der Person verglichen werden, die den biometrischen Pass vorweist. Für diesen Vergleich können die Daten ohne jede Berührung vom Chip abgerufen werden, der im Innern des Passes angebracht ist.

Damit eröffnen sich neue Dimensionen auf dem Gebiet von Ausweisschriften. Die neue Technologie birgt jedoch auch Gefahren. Deshalb ist dem Datenschutz grosses Gewicht beizumessen und die Zugriffsmöglichkeiten auf die eingespeicherten Daten auf das Nötigste zu beschränken sowie vor unerlaubten Zugriffen Dritter zu schützen. Dies insbesondere auch im Hinblick auf die noch künftig zu abschliessenden Verträge und Ermächtigungen seitens des Bundesrates.

Der Bundesrat hat in den beiden vorgelegten Entwürfen zur Abänderung des Ausweisgesetzes sowie der Ausweisverordnung in sehr knapper Form aufgenommen, wer in der Schweiz welche biometri-

schen Daten im biometrischen Pass erfasst, wo diese gespeichert werden und welche schweizerischen Behörden und sonstige Stellen Zugriff haben sollen.

Dabei sind viele Fragen noch unbeantwortet: Ist und falls ja, wie ist die RFID-Chiptechnologie im Ausweis einsetzbar? Gibt es andere, weniger risikobehaftete Technologien anstelle des RFID-Chips? Weshalb möchte der Bundesrat biometrische Daten im ISA speichern? Welche biometrischen Technologien gerade bezüglich Fingerabdrücke und/oder Irismuster will der Bundesrat einsetzen, zumal in diesem Bereich verschiedene Technologien unausgereift sind? Welche hohe Sicherheit garantierende Verschlüsselungstechnologien sollen in der PKI eingesetzt werden, damit Datenmissbrauch, Zweckbehandlungsänderungen etc. von vorne herein ein Riegel geschoben wird?

Es genügt nicht, sich mit Verweisen auf die ICAO oder die EU abzusichern. Der Bundesrat hält selbst fest, dass die Mindestanforderungen der ICAO, insbesondere hinsichtlich des Datenschutzes, den schweizerischen Anforderungen an einen qualitativ hochwertigen Pass nicht genügen (siehe Erläuterungen, Ziff. 4, S. 14).

Nicht geregelt wird die Frage nach den Zugriffsberechtigungen im Ausland und wie die Schweiz allfälligen Missbräuchen dieser Zugriffsberechtigten und anderer (ausländischer) Dritter begegnen will. Dies ist gerade von wesentlicher Bedeutung für Staaten, welche kein mit der Schweiz vergleichbares Datenschutzniveau aufweisen (z. B. USA). Die Befugnis des Bundesrates, Verträge über das Lesen und die Kontrolle der Ausweise, die mit einem Chip ausgestattet sind, abzuschliessen, wird diesbezüglich als ungenügend erachtet. Unzulässige Eingriffe in die Grundrechte der Privatsphäre, des Rechts auf informationelle Selbstbestimmung sowie der persönlichen Freiheit sind zu wahren.

Mangels detaillierterer Kenntnisse kann die vorliegende Vernehmlassung daher nur vorläufigen Charakter haben und muss allgemein bleiben. Es ist deshalb wünschenswert, sobald Ergebnisse des Pilotprojekts vorliegen, erneut eine Vernehmlassung bei den Kantonen und den interessierten Kreisen durchzuführen.

## **2. Stellungnahme zum Vorentwurf des Ausweisgesetzes (VE AwG)**

### **Art. 2 Abs. 1bis Inhalt des Ausweises**

Biometrische Ausweise sind nach dem gegenwärtigen Stand der Technik weder fälschungssicherer noch verifizieren sie deren Inhaber eindeutiger als herkömmliche Ausweise. Fingerabdrücke und Irismuster sind daher als biometrische Daten in den biometrischen Ausweis – auch im Pilotprojekt – wenn überhaupt, erst aufzunehmen, wenn datenschutzfreundliche Technologien und ausgereifte technische Normen/Standards erwiesenermassen eingesetzt werden können. Im weiteren sind Alternativen für jene 2% der Bürgerinnen und Bürger, für welche diese Technik nicht einsetzbar ist, aufzunehmen (Art. 14a Abs. 4 VE VAwG). Auf jeden Fall ist auf die Aufnahme von Fingerabdrücken und/oder Irismuster im biometrischen Pass gänzlich zu verzichten, wenn die entsprechenden Nachweise nicht erbracht werden können. Diese beiden biometrischen Merkmale wären in diesem Fall aus Abs. 1bis zu streichen.

Ein allfälliger Einsatz biometrischer Ausweise ist strikte auf die Verifikation (1:1-Vergleich) der Ausweisinhaber zu beschränken, wie es die geltende Regelung in Art. 1 Abs. 2 AwG bezweckt. Gemäss dieser Bestimmung dienen Ausweise der Inhaberin oder dem Inhaber zum Nachweis der Schweizer Staatsangehörigkeit und der eigenen Identität. Es geht hier also nicht um den Abgleich, ob Herr X identisch mit irgendeiner Person ist (Identifikation 1:n-Vergleich).

Es dürfen nur Templates und nicht Rohdaten der angeführten biometrischen Merkmale im biometrischen Ausweis gespeichert werden. Rohdaten enthalten in jedem Fall viel mehr Zusatzinformationen als das daraus gewonnene Template. Z.B. können aus dem Gesichtsbild (Rohdaten) Zusatzinformationen wie Hinweise auf Geschlecht, Alter, Ethnie, Aussehen, Stimmung, Krankheiten gewonnen werden. Dadurch werden zweckwidrige Datenbearbeitungen und -auswertungen ermöglicht. Die Speicherung von Rohdaten ist nicht notwendig und deshalb unverhältnismässig. Templates genügen zum Zweck der Verifikation vollkommen. Rohdaten sind unverzüglich zu vernichten, sobald Templates und Prüfmuster erstellt sind. In Art. 2 Abs. 1bis ist daher unabhängig davon, welche biometrischen Merkmale zum Einsatz kommen, zu ergänzen, dass ausschliesslich Templates im biometrischen Ausweis gespeichert werden.

Die Speicherung von Templates von Fingerabdrücken und/oder Irismustern ist auf die Sphäre des Nutzers (AusweisinhaberIn) zu beschränken. Deren Speicherung im ISA ist unverhältnismässig, verletzt den aus BV 13 Abs. 2 fliessenden Grundsatz der Datenvermeidbarkeit und wird neue Begehrlichkeiten auf Zugriffe und damit zweckwidrige Datenbearbeitungen nach sich ziehen. Es ist zu prüfen, ob nicht andere Speichermedien anstelle der heiklen RFID-Chiptechnologie eingesetzt werden können. Mittels Einsatz datenschutzfreundlicher Technologien ist zumindest sicherzustellen, dass durch den Einsatz der RFID-Chips nicht unberechtigte Dritte auf die gespeicherten biometrischen Templates zugreifen und zweckwidrig weiterbearbeiten oder gar manipulieren können (siehe Artikel-19-Datenschutzgruppe, Arbeitspapier vom 19.01.2005 über „Datenschutzfragen im Zusammenhang mit der RFID-Technik“).

#### **Art. 2a Speicherung der Daten im Ausweis**

Gemäss dem Grundsatz der Datenvermeidbarkeit ist auf die Speicherung der übrigen Daten im Datenchip zu verzichten (Abs. 2). Eine solche ist in keiner Weise notwendig, da deren Speicherung in maschinenlesbarer Form im Ausweis vollkommen genügt.

Wie bereits angeführt, müssen Technologien eingesetzt werden, welche datenschutzfreundlich sind und hohen Sicherheitsanforderungen genügen. Sonst kann dem erheblichen Missbrauchsrisiko zweckwidriger Zugriffe nicht wirkungsvoll begegnet werden. Deshalb sind unbedingt detailliertere Ausführungen zur zum Einsatz kommenden PKI in die Erläuterungen aufzunehmen.

Das Lesen und Zugreifen auf die im Chip gespeicherten biometrischen Templates ist eine Datenbekanntgabe von Personendaten. Im Vorentwurf müssen daher die schweizerischen datenschutzrechtlichen Vorgaben ausdrücklich geregelt werden und in den völkerrechtlichen Verträgen ist ein entsprechender Vorbehalt betreffend Einhaltung der schweizerischen Datenschutzgesetzgebung anzubringen. Abs. 4 ist um diesbezügliche datenschutzrechtliche Bestimmungen zu ergänzen.

Zu streichen ist in Abs. 4 die Ermächtigung von Transportunternehmen auf die im Chip gespeicherten biometrischen Daten, zuzugreifen. Damit wird das Verhältnismässigkeitsprinzip verletzt. Diese können die Verifikation der Passagiere auf andere Weise vornehmen (z.B. nicht automatisierter 1:1-Vergleich des maschinenlesbaren Ausweises beim Check-In).

#### **Art. 5 Abs. 1**

In der vorgelegten Entwurfsversion sind die Einwohnergemeinden nicht mehr explizit als antragstellende Behörde erwähnt, den Kantonen steht es frei, entsprechende Stellen zu bezeichnen. Die Kantone können somit bestimmen, ob die Zuständigkeit der Einwohnergemeinden als antragstellende Behörden erhalten bleibt.

Das Verfahren kann auf diese Weise vereinfacht werden und direkt die ausstellende Behörde als Stelle bezeichnet werden, welche die Aufgaben der Einwohnergemeinden im Passwesen als Kompensation für eine ehemalige Monopolaufgabe übernimmt, zumal sämtliche Daten aller in der Schweiz lebenden Personen in einem elektronischen System, dem INFOSTAR, erfasst sein werden. Die neue Regelung ermöglicht es aber auch, dass Ausweis-anträge schliesslich nur noch via Biometrieerfassungszentren verarbeitet werden. Die politische Diskussion ist dabei nicht zu unterschätzen, zumal es im Kanton um nicht geringe Gebühreneinnahmen geht.

#### **Art. 6a Ausfertigungsstellen**

Nebst den bereits angeführten hohen Sicherheitsanforderungen ist ein Datenschutzaudit bei den sich bewerbenden (privatrechtlichen) Unternehmen zwingend vorzuschreiben und vorzunehmen. So kann von vornherein Gewähr geboten werden, dass nur eine Unternehmung oder Unternehmungen für die Herstellung biometrischer Ausweise den Zuschlag erhalten, welche über ein hohes Datenschutzniveau verfügen. Art. 6a ist deshalb zu ergänzen, dass jede Bewerberin, jeder Bewerber zur Durchführung eines Datenschutzaudits verpflichtet wird.

#### **Art. 9 Haftung**

Für eine bessere Verifikation (1:1-Vergleich) einer Ausweisinhaberin, eines Ausweisinhabers sind gemäss den gegenwärtigen Erkenntnissen biometrische Daten nicht geeigneter und notwendig. Unausgereifte technische biometrische Verfahren im Bereich Fingerabdrücke und Irismuster führen gerade zum Gegenteil und machen den Ausweis nicht fälschungssicherer resp. verifizieren den Inhaber nicht besser als bereits im Einsatz stehende Ausweise. Die Bürgerin und der Bürger muss sich zudem darauf verlassen können, dass die von ihm beantragten und erhaltenen biometrischen Ausweise hohen Sicherheitsansprüchen entsprechen und Missbräuche auf ihre Privatsphäre und ihr Recht auf informationelle Selbstbestimmung ausgeschlossen werden. Dies gilt unabhängig davon, ob die Bürgerin, der Bürger freiwillig einen biometrischen Pass beantragt oder nicht. Der Bund ist und bleibt für den Datenschutz und die Datensicherheit verantwortlich (Art. 16 des eidg. Datenschutzgesetzes), gleichgültig ob er seine Aufgaben an Dritte delegiert (z.B. Ausfertigungsstellen).

Man stelle sich beispielsweise vor, einer Bürgerin, einem Bürger wird im Staat X die Einreise verweigert, weil sie, ihn das Lesegerät nicht verifizieren kann oder verifiziert. Wer bezahlt den Schaden der hinfälligen Ferienreise oder den nicht zustandegewonnenen Auftrag in Millionenhöhe? Oder wenn dieselbe Bürgerin, derselbe Bürger auf Grund einer unzulässigen Identifikation (1:n-Vergleich) mit in einem Informationssystem gespeicherten biometrischen Daten zufälligerweise einer „Terroristin“, einem „Terroristen“ ähnelt und unverzüglich verhaftet wird und dann erst noch keine Rechtsmittel dagegen ergreifen kann.

Angesichts dieses erheblichen Risikopotentials für die Persönlichkeitsrechte und die persönliche Freiheit geht es nicht an, dass der Bund noch eine Haftung gänzlich ausbedingt. Daran vermag auch nicht die Funktionskontrolle bei der Biometrie-kontrollstelle (Art. 27a VAWG) und der kostenlose Ersatz eines fehlerhaften, unvollständigen oder beschädigten Ausweises (Art. 52 Abs. 1 VAWG) zu ändern, da damit materielle und immaterielle Schäden im vorgenannten Sinne gar nicht abgedeckt sind.

Das Gesetz sieht eine völlige Ausschliessung der Staatshaftung des Bundes vor für Schäden, die durch den Gebrauch eines Ausweises einer Privatperson entstehen. Wie bereits oben ausgeführt, kann die Haftung aber nicht auf die Bürgerinnen und Bürger abgewälzt werden. Bei einem sachge-

rechten Gebrauch des Ausweises durch eine Privatperson ist der Bund für die problemlose Nutzung des Ausweises verantwortlich. Art. 9 VE AwG ist daher ersatzlos zu streichen.

#### **Art. 11 Abs. 1 Informationssystem**

Abs. 1 ist dahingehend zu ändern, dass im ISA keine Fingerabdrücke und/oder Irismuster gespeichert werden (siehe Bemerkungen zu Art. 2 Abs. 1bis VE AwG, S. 2f.).

#### **Art. 12 Datenbearbeitung und Datenbekanntgabe**

Da die Speicherung biometrischer Daten im ISA unzulässig ist, muss Art. 12 weder geändert noch ergänzt werden. Templates biometrischer Daten sind einzig im biometrischen Ausweis zu speichern. Art. 12 ist daher ersatzlos zu streichen (siehe Bemerkungen zu Art. 2 Abs. 1bis VE AwG, S. 2f.).

#### **Art. 16 Vollzug**

Wie bereits angeführt, muss der Vollzug unter strikter Einhaltung der schweizerischen Datenschutzgesetzgebung erfolgen. In Art. 16 ist daher ein ausdrücklicher Vorbehalt einzufügen.

### **3. Stellungnahme zum Vorentwurf der Ausweisverordnung (VE VAWG)**

#### **Art. 6 Ordentliche Ausweise und biometrische Pässe**

Der bisher in Art. 5 AwG gemachte Verweis auf die Wohnsitzgemeinde als Stelle, die ermächtigt ist, Anträge auf Ausstellung eines Ausweises entgegenzunehmen, ist gestrichen worden. Gemäss Art. 6 VE VAWG bestimmen die Kantone die Stellen, bei denen Schweizer Bürgerinnen und Bürger einen Antrag auf einen Ausweis einreichen können. Folglich ist Art. 6 Abs. 1 VE VAWG in diesem Sinne abzuändern und der Anfangssatz „Antragstellende Behörde im Inland ist die Wohnsitzgemeinde“ ... aufzuheben

#### **Art. 14a Inhalt des biometrischen Passes**

Wie bereits angeführt, ist in den Erläuterungen zu ergänzen, wie konkret PKI in biometrischen Verfahren und RFID-Chiptechnologie eingesetzt werden kann. Auf die Aufnahme von Fingerabdrücken im Chip ist gänzlich zu verzichten, wenn keine Alternativen für rund 2 % der Bevölkerung gefunden werden (siehe Bemerkungen zu Art. 2 Abs. 1bis VE AwG, S. 2f.). Zu streichen ist die Zugriffsmöglichkeit von Transportunternehmen auf die im Chip gespeicherten Daten (siehe Bemerkungen zu Art. 2a VE AwG, S. 3).

#### **Art. 17a Zusätzliches Verfahren für den biometrischen Pass**

Dass das Biometrieerfassungszentrum digitale Gesichtsbilder und Fingerabdrücke im ISA erfasst, ist ersatzlos zu streichen, weil die Erfassung und Speicherung dieser biometrischer Templates im ISA nicht verhältnismässig und daher rechtswidrig ist (siehe Bemerkungen zu Art. 2 Abs. 1bis VE AwG, S. 2f.).

#### **Art. 27a Haftung**

Diese Bestimmung ist ersatzlos zu streichen (siehe Bemerkungen zu Art. 9 VE AwG, S. 3f.).

#### **Art. 28 Bst. a**

Diese Bestimmung ist ersatzlos zu streichen, soweit ISA der Überprüfung der biometrischen Daten nach Art. 14a Abs. 1 betrifft (siehe Bemerkungen zu Art. 2 Abs. 1bis VE AwG, S. 2f.).

#### **Art. 30 Abs. 2**

Da im ISA aus datenschutzrechtlicher Sicht keine biometrischen Daten zu speichern sind, ist die genügende Regelung im geltenden Abs. 2, wonach die Verifikation über die Ausweisnummer erfolgt, beizubehalten. Für eine Änderung von Art. 30 Abs. 2 besteht kein Handlungsbedarf.

#### **Art. 37a Informationssystem für die Biometriekontrollstellen**

Dieses Informationssystem muss hohen Sicherheitsanforderungen entsprechen. Es ist zu präzisieren, mit welchen technischen und weiteren organisatorischen Massnahmen die Datensicherheit und die Persönlichkeitsrechte der Bürgerinnen und Bürger vor Missbräuchen effektiv geschützt werden.

#### **Art. 52 Abs. 1, 2bis, 4 und 5 Kostenübernahme bei Mängeln und Versäumnis der Zustellfrist**

Wie bereits angeführt, liegt – auch in der Pilotphase – die Verantwortung für Mängel biometrischer Ausweise ausschliesslich beim Bund, auf jeden Fall nicht bei der Bürgerin, beim Bürger, welche die Ausstellung eines solchen Ausweises beantragt. Bei Erhalt des biometrischen Ausweises muss die antragstellende Person daher Gewähr haben, dass dieser nicht mangelbehaftet ist, gerade weil er technische Mängel im Chip „auf einen Blick“ gar nicht erkennen kann. Deshalb muss die Biometriekontrollstelle von sich aus automatisch vor Zustellung des biometrischen Ausweises die Funktionskontrolle durchführen und der antragstellenden Person schriftlich bestätigen, dass ihr biometrischer Ausweis keine Mängel hat. Im übrigen muss der Ausweisinhaber, dem Ausweisinhaber jederzeit und nicht nur während der 10-tägigen Frist nach Erhalt ein mangelhafter biometrischer Ausweis kostenlos ersetzt werden. Die Abwälzung des Risikos technisch nicht einwandfrei funktionierender biometrischer Ausweise auf die Bürgerin, den Bürger ist nicht bürgerfreundlich und wird zur Nichtakzeptanz des biometrischen Ausweises führen.

Abs. 1 ist deshalb dahingehend zu ändern, dass die Biometriekontrollstelle die Funktionskontrolle vor Zustellung des biometrischen Ausweises an die antragstellende Person vornimmt, die volle Funktionsfähigkeit der antragstellenden Person schriftlich bestätigt und nach Zustellung ein kostenloser Ersatz jederzeit vornimmt, wenn der biometrische Ausweis mangelhaft ist.

#### **Anhang 1 Zugriffsmatrix**

Die neuen Datenfelder digitale Fotografie und Fingerabdrücke sowie die diesbezüglichen Zugriffsberechtigungen im ISA sind ersatzlos zu streichen.

Wir laden Sie ein, unsere Überlegungen im Rahmen der weiteren Behandlung dieses Geschäftes angemessen zu berücksichtigen.

IM NAMEN DES REGIERUNGSRATES

**Regierungsrat**

sig  
Rathaus / Barfüssergasse 24  
Walter Straumann  
Landammann  
[www.sg.ch](http://www.sg.ch)

sig.  
Dr. Konrad Schwaller  
Staatschreiber