Lutz Hasse, Katrin Böhlke

Factum nebulosum – Jus nebulosum

ePass und ePA: Schillernde Datenschutzketten und ihre schwächsten Glieder

Schöner Schein

Seit November 2007 zieren den ePass die biometrischen Merkmale Foto und Fingerabdruck und es laufen auf Bundesebene Vorbereitungen zur Einführung des ePA (ePersonalausweises) am 01.10.2010, natürlich mit den gleichen Biometriefunktionen, z. T. fakultativ.

Solcherlei Errungenschaften werden der umsetzungspflichtigen Basis – wenngleich mit einjähriger Verspätung – denn auch schmackhaft gemacht mit 22 Seiten einer schicken BSI-Handreichung. Deren den Erwartungshorizont nur blass ausmalende Lektüre lässt den beflissenen Leser Empfehlungen entdecken, die möglicherweise die beunruhigten Gewissen der Verfahrensinitiatoren sedieren sollen, indes eines ganz gewiss nicht vermögen: Die Basis, also insbesondere die kleineren Kommunen, in die Lage zu versetzen, aus eigener Kraft die auf sie abgewälzten datenschutzrechtlichen Umsetzungsprobleme zu bewältigen. Diese Probleme sind – wie im Folgenden aufzuzeigen sein wird – komplexer Natur. Ihre Lösungen dürfen nicht allein den Kommunen überlassen bleiben, die personell und finanziell an der unteren Grenze des Machbaren agieren. Vielmehr – so das Petitum dieses Beitrags – sollten die bundesweiten Verfahren von Standards flankiert werden, die eine robuste Kette des Datenschutzes gewährleisten und nicht – wie bisher – solitäre Problemlösungsstrategien begünstigen, bei denen das Reißen schwacher Kettenglieder vorprogrammiert ist. Diese Probleme sind im Einzelnen:

Vertraulichkeit

Gemäß § 6a Abs. 1 PassG sind bei der Datenübermittlung von den Passbehörden an den Passhersteller dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren einzusetzen. Näheres regelt die PassDEÜV; danach werden die zu übertragenden Daten verschlüsselt und signiert in der Bundesdruckerei empfangen. Allerdings können die Originale aller Antragsdaten weiterhin unverschlüsselt und unsigniert und insoweit ungeschützt in den Passbehörden lagern, wie Datenschutzbeauftragte festgestellt haben. Warum?

§ 6a Abs. 2 PassG fordert eine Qualitätssicherung der Fingerabdrücke durch die vom BSI zertifizierten Fingerabdruckerfassungsgesetze. Die Kommunen haben sich darauf verlassen, diese Daten würden dann (natürlich) dem Stand der Technik auch entsprechend vom BSI verschlüsselt und signiert werden. Mithin wurde nicht nur die Sicherung der Qualität, sondern auch des Verfahrens erwartet. Ein Jahr später wurden die Kommunen mit der „Handreichung Informationssicherheit für deutsche Passbehörden“ über ihren Irrtum aufgeklärt: Sie selbst sollten die Daten verschlüsseln, da anderenfalls die Betroffenen erheblich beeinträchtigt und die Passbehörden einen andauernden Imageverlust erleiden können – so das BSI. Hier wird sich – wenn überhaupt – ein bunter Strauß von Verschlüsselungsprogrammen unterschiedlichster Qualität entfalten – zu Lasten der Datensicherheit.

Wie erwähnt werden die Fingerabdrücke bei der Erfassung nicht sofort signiert, sodass bewusste oder unbewusste Veränderungen in den Passbehörden nicht erkannt werden können. Bei der Passrückgabe erfolgt lediglich eine optische Darstellung von 2 Fingerabdrücken, die auch dem daktyloskopisch Minderqualifizierten den Eindruck vermitteln soll, diese stammten vom Antragsteller.

Zunächst der TLfD und sodann die anderen Datenschutzbeauftragten des Bundes und der Länder sehen allerdings Artikel 4 der EG-Verordnung 2252/2004 als nicht erfüllt an, der das Recht einräumt, die in dem Pass gespeicherten personenbezogenen Daten mit aktuell genommenen *überprüfen*, d. h. abgleichen zu können.

Dieses Recht bleibt dem Bürger derzeit verwehrt, weil die Dokumentenlesegeräte diesen Abgleich nicht leisten, deren „Update“ durch den Bund aber noch auf sich warten lässt. Allein Sicherheitsbehörden ist der Abgleich möglich – mit den u. U. unliebsamen Folgen für den Betroffenen.

Löschung

Die Fingerabdrücke sind spätestens nach Aushändigung des Passes zu löschen (§ 16 Abs. 2 PassG). Bei abgebrochener Antragsstellung oder bei während der Ausgabezeit verstorbenen Bürgern oder wenn das Dokument nicht abgeholt wird bleiben die Daten mangels bereichsspezifischer Regelung für unbestimmte Zeit im System. § 21 PassG i.V.m. § 5 PassG dürfte nicht greifen, denn diese Löschfrist sieht nur die Daten im Passregister vor, deren Bestandteil der Fingerabdruck jedoch gerade nicht ist.

Landesdatenschutzgesetze regeln zwar, dass Daten zu löschen sind, sobald sie zur Aufgabenerfüllung nicht mehr erforderlich sind; das Ergebnis dieser Erforderlichkeitsprüfung kann indes sehr wenig einheitlich ausfallen, so dass auch hier zentrale Vorgaben sinnvoll erscheinen.

Fazit

Um die Verfahren datenschutzsicher zu verketteten, ist *bundeseinheitlich* nachzurüsten bei:

- ♦ der Verschlüsselung und Signierung,
- ♦ der Möglichkeit zum Datenabgleich
- ♦ und der Regelung der Löschfristen.

Auch der ePersonalausweis soll die Biometriefunktion beinhalten, die auf einem kontaktlosen Chip mit digitalem Passfoto und zwei Fingerabdrücken basiert; ob bis dahin die erwähnten Probleme behoben sein werden, wird sich zeigen.

MR Dr. Lutz Hasse,
Dipl.-Ing. Katrin Böhlke
Thüringer Landesbeauftragter für den Datenschutz