

Übersicht: Der elektronische Personalausweis – neue Pflichten und Regeln

18. Juni 2010 Rechtsreferendar [Jens Ferner](#) (Diplom-Jurist)

Der elektronische [Personalausweis](#) kommt – und mit ihm nicht nur datenschutzrechtliche bzw. persönlichkeitsrechtliche Diskussionen, sondern auch gesetzliche Änderungen, die die alltägliche Praxis in vielerlei Hinsicht berühren. Einige ausgesuchte Stellen – mit einem Hinweis, warum man ganz genau hinsehen muss, wenn in Gesetzen nur ein einzelnes Wort geändert wird. Und speziell auf die neuen Pflichten von Ausweisinhabern sollte man einen Blick werfen.

Hinweis: Zum Thema [beachten Sie bitte auch den Hinweis](#), dass unsererseits Verfassungsbeschwerde wegen der Volkszählung 2011 eingelegt wurde.

Bis heute verbreitete Praxis und Unsitte ist es, den [Personalausweis](#) als “Pfand” einzufordern. Insbesondere Minderjährige lassen sich hier oft nötigen. Mit dem neuen Personalausweisgesetz ist damit endgültig Schluss, denn dieses normiert im §1:

Vom Ausweisinhaber darf nicht verlangt werden, den [Personalausweis](#) zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben.

Anders als noch im Regierungsentwurf vorgesehen, wird bei einem Verstoß aber kein Bußgeld verhängt. **Wichtig:** speziell manche Dorf-Diskotheken werden hier überlegen müssen, wie sich ein wenig seriöser verhalten können in Zukunft. Diese Regelung hat allerdings einen handfesten Hintergrund, der keinesfalls unterschätzt werden darf: Der neue [Personalausweis](#) beinhaltet neben den ohnehin sensiblen Informationen in bekannter Form nun auch (auf Wunsch) biometrische Merkmale und Daten zur elektronischen Identifikation. **Das Risiko des Identitätsdiebstahls wird damit noch einmal verstärkt.** Allerdings ist es ein Irrtum, zu glauben, dass das Problem nur beim neuen Ausweis mit diesen zusätzlichen Daten gilt – auch ein herkömmlicher Ausweis kann, in den falschen Händen, zu einer finanziellen Bedrohung, mindestens zu einem starken Ärgernis werden. Die Pflicht gilt ab 16 Jahren, bis dahin wird ein Ausweis auf Antrag ausgestellt. Kinder müssen dabei selbst unterschreiben, sobald sie das 10. Lebensjahr vollendet haben (§9 V).

Weiterhin gilt in Deutschland, dass man einen Ausweis besitzen und auf Verlangen vorlegen muss – aber nicht immer bei sich führen muss.

Im neuen Personalausweisgesetz steht nun an zentraler Stelle, was sonst in Ausführungsgesetzen der Länder stand: Ausweise sind Eigentum der Bundesrepublik Deutschland (§4).

Neu ist nun, dass auf Antrag – also nur wenn man es selber möchte – Fingerabdrücke erfasst werden (§5 IX). Eine Rolle spielt der Fingerabdruck zur Zeit im Alltag (noch) nicht. Das neue Personalausweisgesetz (PAG) sieht im §17 eine praktische Regelung vor: Eine prüfende Behörde kann den Fingerabdruck desjenigen der den Ausweis mit sich führt mit dem auf dem Ausweis gespeicherten Abdruck vergleichen, um sicherzustellen, dass Inhaber und im Ausweis benannte Person identisch sind. **Fingerabdrücke werden bei der Personalausweisstelle gespeichert und sind unmittelbar nach Ausstellung des Ausweises zu löschen (§26 II).**

Umfassend geregelt ist die “digitale Identifikation” im §10: Auf Antrag (also wieder nur

freiwillig) wird diese Funktion im [Personalausweis](#) "eingeschaltet". Danach kann man den Ausweis nutzen, um sich digital – etwa mit Kartenleser im Internet – zu identifizieren.  existiert eine Sperrliste, wenn ein Ausweis mit derartiger Funktion abhanden kommt, kann er gesperrt werden und jeder Diensteanbieter ist verpflichtet, den Ausweis vor Nutzung mit der Sperrliste abzugleichen.

Rechtspolitische Anmerkung: An dieser Stelle sollte man ein wenig Weitblick pflegen: Ich finde es nicht abwegig, daran zu denken, dass in naher Zukunft eine "Fahndungsliste" existiert. Wenn dann ein Ausweis elektronisch genutzt wird, der auf dieser Liste steht, wird dies mit einer Lokalisation verbunden. Dieses kurze Szenario zeigt, an welche Chancen und Risiken man bei dem Schritt hin zum elektronischen [Personalausweis](#) denken muss.

Für die Nutzung der elektronischen Identitätsfunktion gibt es eine Geheimnummer (ähnlich der PIN von EC-Karten), ein Sperrkennwort und ein Entsperrkennwort. Diese Daten erhält der Antragsteller (wie bei der EC-Karte) in einem gesonderten Schreiben (§13), das entsprechend vorsichtig aufzubewahren ist.

 Auch hier muss man langsam und schrittweise sein Denken umstellen: Es wird nur eine mittelfristige Frage sein, bis erste Verträge im Internet mit gestohlenen Personalausweisen zustande kommen – wobei vielleicht der Inhaber sein Passwort notiert in der Geldbörse dabei hatte, die insgesamt gestohlen wurde. Die Analogie zu EC-Karten drängt sich wieder einmal auf. Auch die Probleme des "Skimmings", des Abfangens von Daten bei Transaktionen in die ein Ausweis involviert ist, werden sicherlich zunehmen.

Gerade auf Grund der erheblichen (Missbrauchs-)Gefahren durch den neuen Ausweis, wurde die Verwendung ausführlicher geregelt. Während das alte Personalausweisgesetz noch mit einem einzigen Paragraphen (§4 PAG a.F.) auskommt, ist im neuen ein ganzer Abschnitt zu finden: Einmal wird die Verwendung gegenüber und durch Behörden in den §§15 bis 17 geregelt, danach die Verwendung gegenüber und durch nicht-öffentliche Stellen in den §§18-20.

Im Bereich der öffentlichen Stellen findet man dabei eine durchaus ungewohnte Zurückhaltung:

 Verknüpfung von Daten, speziell anhand der Seriennummer des Ausweises, ist untersagt.  automatische Abruf von Daten ist im §15 begrenzt auf Grenzkontrollen, Überwachung durch den Zoll und Fahndung. Die Identitätsfeststellung gegenüber Behörden ist im §17 sehr klar und eng umrissen mit einer ausnahmslosen Löschpflicht "unverzögerlich" nach Ende des Vorgangs.

Die nicht-öffentlichen Stellen können im Zuge des §18 bei der elektronischen Identifikation auf die im Geschäftsverkehr üblichen Daten (Name, Wohnort, Geburtstag etc.) des Ausweisinhabers zugreifen, ausgenommen sind also Seriennummer, biometrische Daten etc. Eine Übermittlung der Daten ist zwingend nur möglich, nach dem der Ausweisinhaber sein Kennwort eingibt (§18 IV) – dabei muss (hier bleibt die Praxis abzuwarten) der Ausweisinhaber in der Lage sein, die zu übermittelnden Daten im Einzelfall auszuwählen (§18 V). Dabei ist es bei einem Bußgeld untersagt, dass eine andere Person als der Ausweisinhaber, den Ausweis benutzt (§18 II). Im Weiteren regelt §20 II ganz deutlich, dass der Ausweis datentechnisch einzig und alleine eine identifizierende Funktion hat:

Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nichtöffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden

Mit Blick auf die Identifikation ist zu Begrüßen, dass der [Personalausweis](#) als "sichere Signaturerstellungseinheit" gilt (§22). Zumindest mittelfristig darf man also auf signierte Mails und sonstige digitale Vorgänge hoffen.

Im Bereich des Registers (die Personalausweisbehörden führen Personalausweisregister), geregelt im §23 – bisher §2a – tut sich so weit nichts neues.

Die Lichtbilder werden ja schon etwas länger hier erfasst, die Fingerabdrücke sind ausdrücklich nicht aufgenommen. Technisch notwendig ist die Aufnahme des Sperrkennwortes, damit jederzeit schnellstmöglich eine Sperrung möglich ist. Hier wird es sicherlich noch Diskussionen geben. Auch beim Zugriff auf Daten des Registers durch andere Behörden (nun §24) hat sich wenig getan. Selbiges beim neuen §25 (vormals §2c), der die Form der Übermittlung von Daten an andere Behörden regelt.  Bei dürfte bisher niemandem aufgefallen sein, dass sich ein Wort im Detail geändert hat: Während der noch gültige §2c PAG den automatisierten Zugriff auf Lichtbilder wegen "Straftaten und Verkehrsordnungswidrigkeiten" ermöglicht, wird im neuen §25 nur noch die Rede sein von "Straftaten und Ordnungswidrigkeiten". Der Anwendungsbereich wird also nicht unerheblich ausgeweitet.

 Ist zu begrüßen, das ausdrücklich festgehalten wird, dass keine zentrale bundesweite biometrische Datenbank angelegt wird (§26 IV). Das Schreckgespenst

bundeslandesweiter biometrischer Datenbanken ist damit freilich noch nicht vom Tisch.

 Probleme ergeben sich beim neuen §27, der die Pflichten des Ausweisinhabers regelt: Während im ersten Absatz die bekannten Pflichten festgesetzt werden (Vorlage bei Behörde bei unrichtigen Daten etc.), haben es die folgenden Absätze in sich. Zum einen wird die Pflicht konstatiert, "zumutbare Maßnahmen" zu treffen, damit Dritte keine Kenntnis von der Geheimnummer erhalten. Darüber hinaus hat man mit dem Absatz 3 dann eine Fülle technischer Pflichten:

Der Personalausweisinhaber soll durch technische und organisatorische Maßnahmen gewährleisten, dass der elektronische Identitätsnachweis gemäß § 18 nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Dabei soll er insbesondere solche technischen Systeme und Bestandteile einsetzen, die vom Bundesamt für Sicherheit in der Informationstechnik als für diesen Einsatzzweck sicher bewertet werden

Was das heißt, liegt wohl auf der Hand: Der heimische PC an dem der Ausweis genutzt wird, muss als "sicher anzusehen sein". Maßstab sind Bewertungen des BSI.  wird also durchaus vom Anwender verlangt, sich über das BSI zu informieren und dann entsprechend Software wie z.B. Antiviren-Software und Firewalls zu nutzen.

Auf Grund von "Sniffing"-Problemen muss man darüber hinaus über die Sicherheit des eigenen Netzwerkes nachdenken, etwa bei "Powerline" ob man sich in einem Mehrparteien Wohnhaus gegen den Zugriff der anderen abgesichert hat – und natürlich ob das eigene WLAN sicher ist. Die Nutzung in Internet-Cafes oder sonst bei Dritten sollte damit ganz außen vor sein, bis eine Zertifizierung solcher externer Möglichkeiten erfolgt.

Viel Arbeit und auch Gefahren kommen hier also auf die Nutzer zu, denn: Sollte etwas schief gehen und ein Vertrag durch einen Dritten geschlossen werden, kann eine Verletzung dieser gesetzlich auferlegten Pflichten zu teuren Konsequenzen führen. Und dabei mag ich nicht einmal unken, inwieweit die Rechtsprechung den bisherigen Anscheinsbeweis von EC-Karten auf elektronische Ausweise übertragen wird (Zur Erinnerung: Bei Bankverfügungen mit gestohlener EC-Karte und PIN geht die Rechtsprechung davon aus, dass der Karteninhaber mit der PIN sorgfaltswidrig umgegangen sein muss).

Im **Fazit** stelle ich fest, dass wohl zu Recht die große Aufregung ob des neuen Personalausweisgesetzes ausgeblieben ist. Man sollte die Entwicklung kritisch, nicht aber unbedingt skeptisch, beobachten. Noch möchte ich aber dringend abraten, die elektronische Ausweisfunktion sofort zu aktivieren – hier bleibt abzuwarten, wie die Entwicklung sich im Alltag abzeichnet, insbesondere wie man dem Betroffenen helfen will, seinen Pflichten einer sicheren Umgebung alltagstauglich nachzukommen. Kritisch stimmt auf jeden Fall, dass im §25 die “Verkehrsordnungswidrigkeiten” durch “Ordnungswidrigkeiten” ersetzt wurden, wobei dies in der Begründung verschleiert wird, durch die Erklärung:

Absatz 2 entspricht im Wesentlichen der Regelung des § 2c Abs. 2 PersAuswG und des § 22a Abs. 2 PassG. Hinzugetreten sind als berechnigte Behörden die Steuerfahndungsstellen der Länder sowie die Behörden der Zollverwaltung.

Die Tatsache, dass Ausweitungen in derart sensiblen Bereichen immer noch “unter den Tisch” gekehrt werden wollen, zeigt, dass man bei jeder Änderungen am Personalausweisgesetz letztlich genau hinsehen muss. Dabei ist zu beachten, dass der aktuelle Ansatz zwar durchaus vertretbar ist, aber letztlich schon sehr grenzwertig. Die Erfahrungen der letzten Jahre zeigen, dass man mit Einführung des elektronischen Ausweises und der damit verbundenen Möglichkeiten genau im Blick haben sollte, welche staatlichen Datenbanken in Zukunft geschaffen werden. Jedenfalls eine Fahndungsdatenbank, die Aktivitäten von Ausweisen “verdächtiger Ausweisinhaber” lokalisiert, ist für mich – zumindest als Forderung – nur noch eine Frage der Zeit.