

## Informationen zum neuen Personalausweis

### Grundlegende Fakten

Der neue Personalausweis wird am 1. November 2010 in Deutschland eingeführt. Ab diesem Datum werden nur noch neue Personalausweise ausgegeben. Alle alten Personalausweise behalten ihre Gültigkeit bis zum Ablaufdatum. Ein vorzeitiger Umtausch ab dem 1. November 2010 ist aber jederzeit möglich.

Das Besondere am neuen Personalausweis ist, dass die auf die Karte aufgedruckten Informationen zusätzlich im Ausweis digital abgelegt werden. Die bekannte Funktion als Sichtausweis bleibt aber vollständig erhalten.

Die Gebühr für die Ausstellung eines neuen Personalausweises ist noch nicht festgelegt.

### Muster, Gestaltung und Sicherheitsmerkmale

Der neue Personalausweis hat die Größe einer Scheckkarte und wird aus Polycarbonat gefertigt. Wie schon der bisherige Ausweis enthält auch das neue Dokument zahlreiche Sicherheitsmerkmale, die die Fälschungssicherheit erhöhen. Unter anderem gehören dazu der Sicherheitsdruck mit mehrfarbigen Guillochen und Mikroschriften, kinografische Strukturen, Oberflächenprägungen, ein integrierter Sicherheitsfaden und ein Laser-Kippbild.

Als neues Datenfeld ist der „Ordens- oder Künstlername“ hinzugekommen.

Bestandteil des neuen Designs ist auch ein Logo auf der Rückseite, das ab November 2010 Internetanwendungen, Automaten und Lesegeräte kennzeichnen wird, die den neuen Personalausweis unterstützen. Die beiden sich ergänzenden Halbkreise stehen für das Prinzip des gegenseitigen Ausweisens zwischen Nutzer und Anbieter und symbolisieren die Verwendung in der Online- und der Offline-Welt.

### Neue Funktionen

Die aufgedruckten Daten werden im Ausweis digital abgelegt. Auf freiwilliger Basis können die Ausweisinhaber auch zwei Fingerabdrücke aufnehmen lassen.

Mit dem berührungslos auslesbaren Ausweis können drei elektronische Funktionen realisiert werden.

Mit der **eID-Funktion** (auch „Online-Ausweisfunktion“) können Dienstleister aus E-Business und E-Government künftig Online-Anwendungen anbieten, bei denen

sich die Nutzer mit ihrem Personalausweis anmelden und registrieren. Auch die Nutzung an Automaten (z. B. zur Altersverifikation) und Zutrittssystemen ist möglich. Nur Dienstleister, die staatliche Berechtigungen beantragt und erhalten haben, können Anwendungen auf Basis der eID-Funktion anbieten. Der Einsatz der eID-Funktion des neuen Ausweises ist sowohl für die Ausweisinhaber als auch für die Anbieter von Diensten freiwillig.

Die **elektronische Signaturfunktion** ist für das rechtsverbindliche Unterzeichnen elektronischer Dokumente und E-Mails vorgesehen. Sie ermöglicht es auf dem digitalen Weg, verbindlich und rechtswirksam Transaktionen durchzuführen, die die Schriftform erfordern.

Personalausweisinhaber können ein entsprechendes Zertifikat für die qualifizierte elektronische Signatur auf den Ausweis nachladen. Ausgeliefert wird der Ausweis immer ohne dieses Zertifikat. Es kann bei Anbietern von Zertifizierungsdiensten, die von der Bundesnetzagentur zugelassen sind, erworben werden.

Die **hoheitliche Ausweisfunktion** ist ausschließlich den zur Identitätsfeststellung berechtigten Behörden, also z. B. Polizei-, Grenz- und Zollkontrollen, vorbehalten. Sie können neben den Angaben zur Person beispielsweise auch auf das Lichtbild und die ggf. erfassten Fingerabdrücke zugreifen.

### **Datenschutz, Datensicherheit und informationelle Selbstbestimmung**

Auf Datenschutz, Datensicherheit und die Wahrung der informationellen Selbstbestimmung wird großer Wert gelegt.

Der neue Personalausweis und die verbundene Infrastruktur ermöglichen:

- die stärkere Bindung zwischen Ausweisinhaber und Dokument
- die valide und sichere Übermittlung von Daten für personalisierte Dienste in E-Business und E-Government
- eine höhere Transparenz und die stärkere Kontrolle der Nutzer über die Verwendung ihrer Daten,
- die pseudonyme Nutzung von Angeboten.

Wirksam verhindert werden:

- das unbemerkte Auslesen von Ausweisdaten,
- das Anlegen von unnötigen oder illegalen Datensammlungen,

- die missbräuchliche Verwendung gestohlener Ausweise,
- die Erstellung von Bewegungs- oder Interessenprofilen,
- das nicht autorisierte Erheben oder Abfangen von personenbezogenen Daten

Alle Informationen und Übertragungen werden mit international anerkannten und etablierten Verschlüsselungsverfahren sicher geschützt. Ein Umgehen der verwendeten Sicherheitsprotokolle und -mechanismen ist mit an Sicherheit grenzender Wahrscheinlichkeit über den gesamten Gültigkeitszeitraum nicht möglich. Ein Zugriffssystem, das auf staatlich vergebenen Berechtigungszertifikaten basiert, regelt darüber hinaus, wer auf welche personenbezogenen Ausweisdaten zugreifen darf. Bevor Daten zwischen einem Lesegerät und einem Ausweis übertragen werden, werden die Echtheit dieser Zertifikate und die Gültigkeit der Berechtigung im Ausweis-Chip geprüft.

Die eID-Funktion basiert auf dem Prinzip des gegenseitigen Authentisierens, wonach beide Seiten auf die angegebene Identität ihres Gegenübers vertrauen können: Nur mit einem staatlich ausgestellten Berechtigungszertifikat ist es Anbietern von Internet- oder Automaten Diensten technisch möglich, auf Ausweisdaten zuzugreifen. In diesem Zertifikat ist auch hinterlegt, welche Datenkategorien der Diensteanbieter abfragen darf. Letztendlich bestimmt aber immer der Nutzer, welche Daten übertragen werden und gibt sie durch die Eingabe einer sechsstelligen PIN frei.

Die ausgetauschten Daten sind somit in jedem Fall für beide Seiten valide. Daten werden ausschließlich zwischen dem Anbieter des Dienstes und dem Ausweisinhaber übertragen. Biometrisch nutzbare Daten, also Lichtbild, ggf. Fingerabdrücke, Augenfarbe, Körpergröße und die eigenhändige Unterschrift, werden in keinem Falle an Diensteanbieter oder über das Internet übertragen.

Die freiwillig abgegebenen Fingerabdrücke werden nur auf dem Ausweis und nicht in Registern oder Datenbanken gespeichert.

Das digitale Lichtbild und die Fingerabdrücke verhindern Missbrauch z. B. an Grenzkontrollstationen und stärken die Bindung zwischen Ausweisdokument und -inhaber.

Nur hoheitliche Stellen verfügen über die Berechtigung und die technische Möglichkeit, diese sensiblen Informationen abzufragen. Zu diesem Zweck müssen die jeweiligen Behörden über spezielle Lesegeräte und hoheitliche Berechtigungszertifikate verfügen.

Der Personalausweischip kann nur aus einer maximalen Entfernung von etwa 15 cm angesprochen werden. Dabei wird ein unbemerktes Auslesen, z. B. aus der Hosentasche und selbst bei Vorliegen eines hoheitlichen Berechtigungszertifikates, sicher verhindert, da zusätzlich zum Berechtigungszertifikat die maschinenlesbare Zone oder die 6-stellige Zugangsnummer des Ausweises bekannt sein muss. Diese sind aber nur auf dem Personalausweis vorhanden.

### Weitere Informationen

„Gesetz über Personalausweise und den elektronischen Identitätsnachweis“:

<http://www.bmi.bund.de/cae/servlet/contentblob/607490/publicationFile/34867/eperso.pdf>

Info auf der Website des Bundesinnenministeriums:

[http://www.bmi.bund.de/cln\\_095/DE/Themen/Sicherheit/PassAusweise/ePersonalausweis/ePersonalausweis\\_node.html](http://www.bmi.bund.de/cln_095/DE/Themen/Sicherheit/PassAusweise/ePersonalausweis/ePersonalausweis_node.html)

Info auf der Website des Bundesbeauftragten für Informationstechnik:

[http://www.cio.bund.de/cln\\_102/DE/IT-Projekte/Leuchtturmprojekt\\_ePA/leuchtturmprojekt\\_eпа\\_node.html](http://www.cio.bund.de/cln_102/DE/IT-Projekte/Leuchtturmprojekt_ePA/leuchtturmprojekt_eпа_node.html)