Bundesrat **Drucksache 240/10**

22.04.10

In

Verordnung
des Bundesministeriums des Innern

Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)

A. Problem und Ziel

Mit der Föderalismusreform ist die Gesetzgebungskompetenz für das Ausweiswesen gemäß Artikel 73 Absatz 1 Nummer 3 des Grundgesetzes vollständig auf den Bund übergegangen. Das auf Grund dieser Kompetenz geschaffene Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18. Juni 2009 (BGBl. I S. 1346) tritt am 1. November 2010 in Kraft. Es erweitert den herkömmlichen Personalausweis zu einem biometriegestützten Identitätsdokument und einem elektronischen Identitätsnachweis für E-Government und E-Business.

§ 34 des Personalausweisgesetzes ermächtigt das Bundesministerium des Innern, in einer Verordnung u.a. die Muster der Ausweise zu bestimmen und Einzelheiten zum Verfahren, zu den technischen Anforderungen der Erfassung, zur Qualitätssicherung, zur Speicherung der Fingerabdrücke und Lichtbilder, zum elektronischen Identitätsnachweis, zum Sperrmanagement sowie zur Vergabe von Berechtigungszertifikaten zu regeln.

B. Lösung

Schaffung der rechtlichen Grundlagen durch eine Rechtsverordnung. Die Rechtsverordnung soll zeitgleich mit dem Inkrafttreten des § 34 des Personalausweisgesetzes am 1. November 2010 ausgefertigt werden.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

C. Alternativen

Keine.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Es entstehen Kosten in derzeit noch nicht bekannter Höhe für die neu zu errichtenden Personalausweisbehörden im Ausland. Da Personalausweise nach dem Gesetz nunmehr erstmals auch im Ausland ausgestellt werden sollen, übernehmen die deutschen Auslandsvertretungen insoweit – anders als die innerdeutschen Personalausweisbehörden – vollständig neue Aufgaben. Die für Visa und elektronische Reisepässe aufgebauten Infrastrukturen werden jedoch teilweise mitgenutzt werden können. Die Auslandsvertretungen haben angesichts der erwarteten Nachfrage nach dem elektronischen Personalausweis auch mit einem Anwachsen der Antragstellerzahlen zu rechnen. Diese zusätzliche Belastung wird in noch nicht absehbarem Umfang Investitionskosten für bauliche Erweiterungen, Anpassungen der IT-Infrastruktur sowie zusätzlichen Personalbedarf (Entsandte, Ortskräfte sowie Personal in der Zentrale) verursachen.

Durch die Verordnung selbst entstehen keine weiteren Haushaltsausgaben ohne Vollzugsaufwand. Diese sind bereits in das Gesetzgebungsverfahren eingeflossen.

2. Vollzugsaufwand

Die Einführung des neuen Personalausweises wird bei den Ausweisbehörden zu einem erhöhten Vollzugsaufwand führen. Dieser wurde bereits im Gesetzgebungsverfahren beschrieben. Die genannten Mehraufwände in den Personalausweisbehörden und bei der Vergabestelle für Berechtigungszertifikate werden durch die Personalausweisgebühr sowie weitere noch festzulegende Gebühren für das Verwaltungsverfahren (insbesondere für Berechtigungszertifikate), gedeckt. Die konkrete Ausgestaltung sowie der Kostendeckungsgrad werden jedoch in einer eigenen Gebührenverordnung geregelt.

Die vom Auswärtigen Amt nach den Bestimmungen des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis und diese Verordnung für die Ausstellung von Personalausweisen im Ausland bestimmten Auslandsvertretungen übernehmen ab dem 1. Januar 2013 ein vollkommen neues

Aufgabenfeld, da Personalausweise bislang nur in Deutschland ausgestellt wurden. Insoweit wird in diesen Behörden ein noch nicht absehbarer Vollzugsaufwand entstehen, welcher auch baulichen und personellen Mehrbedarf bedingen wird.

E. Sonstige Kosten

Der Wirtschaft entstehen ggf. Kosten für Berechtigungszertifikate und Lesegeräte, sofern sie den elektronischen Identitätsnachweis nutzen möchte. Diesen Kosten stehen aber zugleich Einsparpotentiale für geringeren organisatorischen Aufwand und ein Gewinn an Sicherheit im Geschäftsverkehr gegenüber, sodass Auswirkungen auf Einzelpreise, das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau, nicht zu erwarten sind. Insbesondere mittelständische Unternehmen werden von dem Verfahren des elektronischen Identitätsnachweises profitieren können.

F. Bürokratiekosten

Die Verordnung enthält 11 Informationspflichten für die Wirtschaft. Für die Bürgerinnen und Bürger sind vier Informationspflichten, für die Verwaltung 13 Informationspflichten enthalten.

Bundesrat **Drucksache 240/10**

22.04.10

In

Verordnung
des Bundesministeriums des Innern

Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)

Der Chef des Bundeskanzleramtes Berlin, den 21. April 2010

An den
Präsidenten des Bundesrates
Herrn Bürgermeister
Jens Böhrnsen
Präsident des Senats der
Freien Hansestadt Bremen

Sehr geehrter Herr Präsident,

hiermit übersende ich die vom Bundesministerium des Innern zu erlassende

> Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)

mit Begründung und Vorblatt.

Ich bitte, die Zustimmung des Bundesrates aufgrund des Artikels 80 Absatz 2 des Grundgesetzes herbeizuführen.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage beigefügt.

Mit freundlichen Grüßen
Ronald Pofalla

Drucksache 240/10

Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)

Vom 1. November 2010

Auf Grund des § 34 des Personalausweisgesetzes vom 18. Juni 2009 (BGBl. I S. 1346) in Verbindung mit dem 2. Abschnitt des Verwaltungskostengesetzes vom 23. Juni 1970 (BGBl. I S. 821), verordnet das Bundesministerium des Innern im Benehmen mit dem Auswärtigen Amt:

Inhaltsübersicht

Kapitel 1	Allgemeine Vorschriften
Kapitel 2	Übermittlung der Ausweisantragsdaten
Kapitel 3	Produktion
Kapitel 4	Aushändigung
Kapitel 5	Änderung von Daten
Kapitel 6	Nutzung des elektronischen Identitätsnachweises
Kapitel 7	Sperrung und Entsperrung des elektronischen Identitätsnachweises
Kapitel 8	Beantragung von Berechtigungen
Kapitel 9	Ausgabe von Berechtigungszertifikaten
Kapitel 10	Schlussvorschriften

Anhang 1	*Muster des Personalausweises*
Anhang 2	*Muster des vorläufigen Personalausweises*
Anhang 3	*Formale Anforderungen an die Einträge im Personalausweis*
Anhang 4	*Übersicht über die Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik*
Anhang 5	*Übersicht über die zu zertifizierenden Systemkomponenten*

Kapitel 1
Allgemeine Vorschriften

§ 1
Begriffsbestimmungen

(1) Eine Sperrsumme ist ein eindeutiges Merkmal, das aus dem Sperrkennwort nach § 2 Absatz 6 des Personalausweisgesetzes, dem Familiennamen, den Vornamen und dem Tag der Geburt eines Ausweisinhabers errechnet wird. Es dient der Übermittlung einer Sperrung vom Sperrnotruf oder einer Personalausweisbehörde an den Sperrlistenbetreiber. Mit Hilfe der Sperrsumme ermittelt der Sperrlistenbetreiber anhand der Referenzliste den Sperrschlüssel eines zu sperrenden elektronischen Identitätsnachweises.

(2) Ein Sperrschlüssel ist ein eindeutiges kartenspezifisches Merkmal, das der Errechnung eines allgemeinen Sperrmerkmals eines zu sperrenden elektronischen Identitätsnachweises dient. Er wird vom Ausweishersteller erzeugt, dem Sperrlistenbetreiber übermittelt und dauerhaft in der Referenzliste gespeichert.

(3) Berechtigungszertifikateanbieter im Sinne dieser Verordnung ist eine natürliche oder juristische Person, die Berechtigungszertifikate im Sinne des § 2 Absatz 4 Satz 1 des Personalausweisgesetzes ausstellt.

(4) Ein allgemeines Sperrmerkmal ist ein eindeutiges kartenspezifisches Merkmal, das einen gesperrten elektronischen Identitätsnachweis in der allgemeinen Sperrliste repräsentiert. Es wird Berechtigungszertifikateanbietern übermittelt, die es zu Sperrmerkmalen nach § 2 Absatz 7 des Personalausweisgesetzes umrechnen.

(5) Der Sperrnotruf ist eine Einrichtung, über die der Ausweisinhaber seinen elektronischen Identitätsnachweis unter Angabe von Sperrkennwort, Familienname, Vornamen und Tag der Geburt in die allgemeine Sperrliste aufnehmen lassen kann.

(6) Extensible Markup Language für hoheitliche Dokumtente (XhD) ist ein in erweiterbarer Seitenbeschreibungssprache (XML) verfasstes Datenaustauschformat für hoheitliche Dokumente.

(7) OSCI-Transport ist der vom Kooperationsausschuss Automatisierte Daten-verarbeitung Bund / Länder / Kommunaler Bereich festgelegte jeweils geltende Standard für ein Datenübermittlungsprotokoll. Der Standard OSCI-Transport ist in der vom Bundesamt für Sicherheit in der Informationstechnik festgelegten Fassung, die im elektronischen Bundesanzeiger bekannt gemacht ist, zu verwenden.

§ 2
Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

Nach dem Stand der Technik sind zu erfüllen

1. die technischen Anforderungen an
   a) die Speicherung des Lichtbildes und der Fingerabdrücke und
   b) den Zugriffsschutz auf die im elektronischen Speicher- und Verarbeitungsmedium abgelegten Daten sowie
2. die technischen und organisatorischen Anforderungen an
   a) die Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke,
   b) die Übermittlung sämtlicher Ausweisantragsdaten von den Personalausweisbehörden an den Ausweishersteller,
   c) den elektronischen Identitätsnachweis und

d) die Geheimnummer, die Sperrung und Entsperrung des elektronischen Identitätsnachweises durch den Ausweisinhaber und die Speicherung und Löschung der Sperrmerkmale und des Sperrkennwortes, insbesondere an die dabei einzusetzenden technischen Systeme und Kommunikationswege.

Der Stand der Technik ist als niedergelegt zu vermuten in den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik. Diese sind in Anhang 4 aufgeführt und gelten in der jeweils im elektronischen Bundesanzeiger veröffentlichten Fassung.

§ 3

Zertifizierung

(1) Die Systemkomponenten der Personalausweisbehörden, des Ausweisherstellers, der Diensteanbieter und ihrer Auftragnehmer nach § 11 des Bundesdatenschutzgesetzes, deren Zertifizierung verpflichtend oder optional ist, ergeben sich aus dem Anhang 5. Die Art und die Einzelheiten der Zertifizierung sind den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zu entnehmen.

(2) Für die Zertifizierung gilt § 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821) sowie die BSI-Zertifizierungsverordnung vom 7. Juli 1992 (BGBl. I S. 1230) in der jeweils geltenden Fassung.

(3) Die Kosten der Zertifizierung trägt der Antragsteller. Die BSI-Kostenverordnung vom 3. März 2005 (BGBl. I S. 519) in der jeweils geltenden Fassung findet Anwendung.

§ 4

Dokumentationspflichten

(1) Die Personalausweisbehörde dokumentiert für die Zwecke des elektronischen Identitätsnachweises:

1. Erklärungen des Ausweisinhabers, die im Rahmen der Antragstellung und Ausweisverwaltung erfolgt sind;
2. das Datum und die Uhrzeit der Ausgabe des Personalausweises;
3. das Datum und die Uhrzeit der Übergabe des Briefes mit der Geheimnummer, der Entsperrnummer und dem Sperrkennwort, falls die Personalausweisbehörde den Brief übergibt;
4. die Ausschaltung des elektronische Identitätsnachweises mit Datum und Uhrzeit der Ausschaltung sowie die Personalausweisbehörde, die den elektronischen Identitätsnachweis ausgeschaltet hat;
5. die Einschaltung des elektronischen Identitätsnachweises mit Datum und Uhrzeit der Einschaltung sowie die Personalausweisbehörde, die den elektronischen Identitätsnachweis eingeschaltet hat;
6. den Sperrantrag durch den Ausweisinhaber, die Übermittlung der Sperrsumme an den Sperrlistenbetreiber sowie das Datum und die Uhrzeit von Antrag und Übermittlung;
7. den Entsperrantrag des Ausweisinhabers, die Übermittlung der Sperrsumme an den Sperrlistenbetreiber sowie das Datum und die Uhrzeit von Antrag und Übermittlung.

(2) Der Sperrnotruf dokumentiert für die Zwecke des elektronischen Identitätsnachweises

den Sperrantrag durch den Ausweisinhaber, die Übermittlung der Sperrsumme an den Sperrlistenbetreiber sowie das Datum und die Uhrzeit von Antrag und Übermittlung.

(3) Der Sperrlistenbetreiber dokumentiert

1. im Zusammenhang mit der Sperrung des elektronischen Identitätsnachweises

a) den Eingang des Sperrantrages mit der Sperrsumme sowie das Datum und die Uhrzeit des Eingangs,

b) die Aufnahme des allgemeinen Sperrmerkmals in die Sperrliste sowie das Datum und die Uhrzeit der Sperrung,

c) die Anfrage zur Erzeugung der Sperrliste sowie das Datum und die Uhrzeit der Erzeugung und

d) den tatsächlichen Abruf sowie das Datum und die Uhrzeit des tatsächlichen Abrufs sowie

2. im Zusammenhang mit der Entsperrung des elektronischen Identitätsnachweises

a) den Eingang des Entsperrantrages mit der Sperrsumme sowie das Datum und die Uhrzeit des Eingangs,

b) die Entfernung des allgemeinen Sperrmerkmals aus der Sperrliste sowie das Datum und die Uhrzeit der Entfernung,

c) die Bereitstellung der Sperrliste zum Abruf sowie das Datum und die Uhrzeit der Bereitstellung sowie

d) den tatsächlichen Abruf sowie das Datum und die Uhrzeit des tatsächlichen Abrufs.

§ 5
Speicherung und Löschung

(1) Für die Speicherung personenbezogener Daten nach dieser Verordnung bei den Personalausweisbehörden gilt § 23 Absatz 4 des Personalausweisgesetzes entsprechend.

(2) Personenbezogene Daten beim Sperrnotruf sind ein Jahr nach ihrer Erhebung zu löschen.

(3) Für die Speicherung beim Sperrlistenbetreiber gelten folgende Fristen:

1. Sperrschlüssel und Sperrsumme sind zehn Jahre nach deren Eintragung aus der Referenzliste zu löschen.
2. Aktualisierungen der Sperrliste werden gespeichert, damit eine Sperrung oder Entsperrung von elektronischen Identitätsnachweisen nachgewiesen werden kann. Sie werden zehn Jahre nach ihrer Speicherung gelöscht.
3. Ein allgemeines Sperrmerkmal wird aus der Sperrliste entfernt zehn Jahre, nachdem der Sperrschlüssel beim Sperrlistenbetreiber gespeichert worden ist, oder wenn die Personalausweisbehörde eine Entsperrung vorgenommen hat.

(4) Der Ausweishersteller speichert die Daten, die im Rahmen des Produktionsverfahrens erlangt oder erzeugt worden sind und der antragstellenden Person zugeordnet werden können, höchstens so lange bis der Sperrlistenbetreiber den Empfang der Sperrsumme und des Sperrschlüssels und die Personalausweisbehörde den Eingang des Sperrkennworts bestätigt haben. Im Übrigen sind die Daten sicher zu löschen.
Der Ausweishersteller führt zur Vermeidung von Doppelungen eine Liste mit Sperrsummen von hergestellten Personalausweisen. Die Sperrsummen in dieser Liste sind zehn Jahre nach ihrer Eintragung zu löschen. § 26 Absatz 3 Satz 1 des Personalausweisgesetzes bleibt unberührt.

Kapitel 2
Übermittlung der Ausweisantragsdaten

§ 6
Erfassung der Anschrift

Der Wohnort in der Anschrift nach § 5 Absatz 2 Nummer 9 Alternative 1 des Personalausweisgesetzes ist mit der allgemeinen Bezeichnung und mit dem im amtlichen Gemeindeverzeichnis verwendeten eindeutigen Gemeindeschlüssel zu erfassen. Zusätze zum Namen des Wohnortes sind einheitlich aufzunehmen, wenn dies für die Eindeutigkeit des Wohnortes oder des Straßennamens erforderlich ist. Darüber hinaus wird auch die Postleitzahl erfasst.

§ 7
Qualitätssicherung des Lichtbildes und der Fingerabdrücke

(1) Bei der Beantragung eines Personalausweises ist von der antragstellenden Person ein aktuelles Lichtbild ohne Rand vorzulegen, das 45 Millimeter hoch und 35 Millimeter breit ist. Wenn die Personalausweisbehörde die technischen Voraussetzungen geschaffen hat, kann das Lichtbild auch

1. von Dritten elektronisch verschlüsselt und signiert an die Personalausweisbehörde übermittelt werden, soweit diese Form der Übermittlung durch eine Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik vorgesehen ist, oder
2. durch die Personalausweisbehörde gefertigt werden.

(2) Die Personalausweisbehörde stellt durch geeignete technische und organisatorische Maßnahmen die erforderliche Qualität der Erfassung des Lichtbildes und der Fingerabdruckbilder sicher. Dazu hat sie die Fingerabdruckbilder und das Lichtbild mit einer zertifizierten Qualitätssicherungssoftware zu prüfen und in dem für den Ausweis verwendeten Format zu speichern. Darüber hinaus hat auch die Erfassung der Fingerabdruckbilder mit zertifizierter Hardware zu erfolgen.

(3) Das Lichtbild muss die Person in einer Frontalaufnahme, ohne Kopfbedeckung und ohne Bedeckung der Augen zeigen. Im Übrigen muss das Lichtbild den Vorgaben des Anhangs 3 Abschnitt 2 entsprechen. Die Personalausweisbehörde kann von diesen Vorgaben aus medizinischen Gründen, die nicht nur vorübergehender Art sind, Ausnahmen zulassen. Vom Verbot der Kopfbedeckung kann sie auch aus religiösen Gründen Ausnahmen zulassen.

§ 8
Übermittlung

(1) Nachdem die Personalausweisbehörde alle Antragsdaten erfasst hat, führt sie diese zu einem digitalen Datensatz zusammen und übermittelt sie dem Ausweishersteller. Die Datenübermittlung umfasst auch

1. die Qualitätswerte zu den Fingerabdrücken, soweit diese abgenommen wurden,
2. die Qualitätswerte zu den Lichtbildern,
3. die Versionsnummern der Qualitätssicherungssoftware,
4. die Sollwerte der Qualitätssicherungssoftware,
5. die technischen Eigenschaften der gespeicherten biometrischen Daten gemäß ISO-Standard 19794,
6. die Behördenkennzahl sowie
7. den Zeitstempel des Ausweisantrags.

Die Datenübermittlung erfolgt entweder durch Datenübertragung über die informationstechnischen Netze von Bund und Ländern oder über allgemein zugängliche Netze. Soweit die Datenübermittlung zwischen informationstechnischen Netzen von Bund und Ländern stattfindet, ist dafür spätestens ab dem 1. Januar 2015 nach § 3 des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder vom 10. August 2009 (BGBl. I S. 2706) das Verbindungsnetz zu nutzen. Die zu übermittelnden Daten sind nach dem Stand der Technik fortgeschritten elektronisch zu signieren und zu verschlüsseln.

(2) Zum Signieren und Verschlüsseln der nach Absatz 1 zu übermittelnden Daten sind geeignete gültige Zertifikate aus der untergeordneten Zertifizierungsinstanz „Hoheitliche Dokumente“ der Deutschland-Online-Infrastruktur zu verwenden.

(3) Für die Übermittlung der Daten an den Ausweishersteller nach Absatz 1 Satz 3 wird das Datenformat XhD auf der Basis des Datenübermittlungsprotokolls OSCI-Transport verwendet. Die Datenübermittlung kann auch über Vermittlungsstellen erfolgen. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; insofern sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren – auch im Fall der Nutzung allgemein zugänglicher Netze – anzuwenden. Das Auswärtige Amt kann für die Datenübermittlung an den Ausweishersteller ein abweichendes Übermittlungsprotokoll verwenden. Die Datenübermittlung zwischen dem Auswärtigen Amt und seinen Auslandsvertretungen muss hinsichtlich Datensicherheit und Datenschutz ein den Anforderungen dieser Verordnung entsprechendes Niveau aufweisen.

(4) Vor der Übermittlung der Ausweisdaten hinterlegen Personal-ausweisbehörden, Ausweishersteller und Vermittlungsstellen alle für eine elektronische und automatisierte Kommunikation benötigten technischen Verbindungsparameter im Deutschen Verwaltungsdiensteverzeichnis (DVDV), insbesondere die dafür erforderlichen Zertifikate. Der Ausweishersteller nutzt eine Funktionalität des DVDV, um die Personalausweisbehörde als eine solche zu verifizieren. Das Auswärtige Amt kann die benötigten technischen Verbindungsparameter und die damit verbundenen erforderlichen Zertifikate technisch unabhängig vom Deutschen Verwaltungsdiensteverzeichnis (DVDV) lösen. Die Lösung muss hinsichtlich Datensicherheit und Datenschutz ein den Anforderungen dieser Verordnung entsprechendes Niveau aufweisen.

§ 9
Qualitätsstatistik

(1) Der Ausweishersteller erstellt eine Qualitätsstatistik. Sie enthält anonymisierte Qualitätswerte zu Lichtbildern und Fingerabdrücken, die sowohl in der Personalausweisbehörde als auch beim Ausweishersteller ermittelt und vom Ausweishersteller in der Qualitätsstatistik ausgewertet und zusammengefasst werden.

(2) Der Ausweishersteller stellt die Ergebnisse der Auswertung und auf Verlangen die in der Statistik erfassten anonymisierten Einzeldaten dem Bundesministerium des Innern, dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundeskriminalamt zur Verfügung.

Kapitel 3
Produktion

§ 10
Eingang der Antragsdaten

Der Ausweishersteller prüft, ob die Antragsdaten vollständig und unversehrt eingegangen sind, und bestätigt der Personalausweisbehörde unverzüglich den Eingang in elektronischer Form. Er hat technische und organisatorische Maßnahmen zu treffen, die ausschließen, dass ungültig oder falsch signierte oder anderweitig fehlerhafte Antragsdaten weiterverarbeitet werden. Der Ausweishersteller prüft die Identität der übermittelnden Personalausweisbehörde.

§ 11
Muster für den Personalausweis

Der Personalausweis ist nach dem in Anhang 1 abgedruckten Muster herzustellen. Für die einzutragenden Daten gelten die formalen Anforderungen des Anhangs 3 Abschnitt 1.

§ 12
Muster für den vorläufigen Personalausweis

Der vorläufige Personalausweis ist nach dem in Anhang 2 abgedruckten Muster herzustellen. Für die einzutragenden Daten gelten die formalen Anforderungen des Anhangs 3 Abschnitt 1.

§ 13
Schnittstelle des elektronischen Speicher- und Verarbeitungsmediums

Das elektronische Speicher- und Verarbeitungsmedium des Personalausweises ist mit einer kontaktlosen Schnittstelle ausgestattet und benötigt für die Datenübertragung die Energieversorgung durch Lesegeräte.

§ 14
Speicherung von personenbezogenen Daten; Zugriffsschutz

(1) Alle im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeicherten personenbezogenen Daten sind gegen unbefugten Zugriff zu schützen. Es ist insbesondere sicherzustellen, dass

1. vor der Übermittlung personenbezogener Daten die Geheimnummer, die Zugangsnummer oder die Daten der maschinenlesbaren Zone (MRZ) eingegeben werden müssen,
2. Zugriffsrechte über Berechtigungszertifikate nachgewiesen werden müssen und
3. alle personenbezogene Daten zwischen dem elektronischen Speicher- und Verarbeitungsmedium und Inhabern von Berechtigungszertifikaten verschlüsselt übermittelt werden.

(2) Der Personalausweis ist so herzustellen, dass personenbezogene Daten ausschließlich ausgelesen werden können durch

1. Behörden, die zur Identitätsfeststellung berechtigt sind und ein hoheitliches Berechtigungszertifikat nutzen, oder
2. berechtigte Diensteanbieter, die ein Berechtigungszertifikat nutzen, nach Eingabe der Geheimnummer durch den Ausweisinhaber.

§ 15
Übermittlung und Übersendung des Sperrkennworts an die Personalausweisbehörde

(1) Der Ausweishersteller übermittelt der Personalausweisbehörde im Datenübertragungsformat XhD auf sicherem elektronischem Weg verschlüsselt und signiert das Sperrkennwort zur Speicherung im Personalausweisregister.

(2) Die Personalausweisbehörde bestätigt dem Ausweishersteller den Eingang des Sperrkennworts unverzüglich. Hat der Ausweishersteller drei Werktage, nachdem er das Sperrkennwort übermittelt hatte, keine Bestätigung erhalten, fragt er bei der Personalausweisbehörde nach.

§ 16
Übermittlung der Sperrsumme und des Sperrschlüssels an den Sperrlistenbetreiber

Der Ausweishersteller übermittelt dem Sperrlistenbetreiber auf sicherem elektronischem Weg verschlüsselt und signiert die Sperrsumme und den Sperrschlüssel eines Personalausweises, bevor er diesen an die Personalausweisbehörde sendet. § 8 Absatz 1 Satz 3 bis 5 gilt entsprechend. Der Sperrlistenbetreiber bestätigt dem Ausweishersteller unverzüglich den Eingang dieser Daten. Hat der Ausweishersteller zwei Werktage, nachdem er die Sperrsumme und den Sperrschlüssel übermittelt hat, keine Bestätigung erhalten, fragt er bei dem Sperrlistenbetreiber nach.

§ 17
Übersendung der Geheimnummer, der Entsperrnummer und des Sperrkennworts

(1) Der Ausweishersteller übersendet der antragstellenden Person die Geheimnummer, die Entsperrnummer und das Sperrkennwort des Personalausweises in einem Brief. Als Absenderanschrift ist die postalische Anschrift der ausstellenden Personalausweisbehörde anzugeben.

(2) Personalausweis und Geheimnummer dürfen zu keinem Zeitpunkt mit gleicher Post versandt werden.

(3) In den Fällen des § 13 Satz 3 des Personalausweisgesetzes soll bis zur persönlichen Übergabe an die antragstellende Person der Schutz gegen Kenntnisnahme der Geheimnummer und der Entsperrnummer durch Dritte gewährleistet sein.

(4) Der Ausweishersteller versendet den Brief nach Absatz 1 an die im Personalausweis angegebene Anschrift. Hat die antragstellende Person keine alleinige Wohnung in Deutschland wird der Brief vom Ausweishersteller nach Weisung des Auswärtigen Amtes, die mit dem Bundesministerium des Innern abgestimmt ist, an die ausstellende Personalausweisbehörde oder aber an die antragstellende Person persönlich versandt. Bei als unzustellbar zurückgesandten Briefen übergibt die Personalausweisbehörde den Brief an die antragstellende Person. Absatz 3 gilt entsprechend.

(5) Der Ausweishersteller erstellt und versendet einen Brief nur dann, wenn die antragstellende Person zum Antragszeitpunkt mindestens 15 Jahre und neun Monate alt ist.

(6) Hat die antragstellende Person den Brief nicht erhalten, kann sie einen neuen Personalausweis beantragen. In diesem Fall wird der zum neuen Personalausweis gehörende Brief an die Personalausweisbehörde versandt, die ihn der antragstellenden Person übergibt. Absatz 3 gilt entsprechend.

(7) Die antragstellende Person muss, bevor ihr der Personalausweis ausgehändigt wird, schriftlich bestätigen, dass sie den Brief auf postalischem Wege oder durch Übergabe empfangen hat. Satz 1 gilt nicht für antragstellende Personen, die keine alleinige Wohnung in Deutschland haben, wenn diesen der Personalausweis nicht persönlich durch die Personalausweisbehörde übergeben wird.

Kapitel 4
Aushändigung

§ 18
Aushändigung des Personalausweises

(1) Erklärt die antragstellende Person, den elektronischen Identitätsnachweis nicht nutzen zu wollen, schaltet die Personalausweisbehörde den elektronischen Identitätsnachweis aus.

(2) Bestätigt die antragstellende Person den Empfang des Briefes nach § 17 Absatz 7 nicht, darf der Personalausweis nur mit ausgeschaltetem elektronischem Identitätsnachweis übergeben werden.

(3) Der Ausweisinhaber kann sich die auslesbaren personenbezogenen Daten, die auf seinem Personalausweis gespeichert sind, jederzeit bei einer Personalausweisbehörde anzeigen lassen.

(4) Für das Lesen der Daten nach den Absätzen 1 und 3 sind zertifizierte Lesegeräte mit hoheitlichem Berechtigungszertifikat zu verwenden.

(5) Die Personalausweisbehörde im Ausland darf Personalausweise im Ausland auf dem Postweg an die antragstellende Person versenden, sofern die Abholung des Personalausweises für die antragstellende Person nur unter unzumutbaren Umständen möglich wäre.

Kapitel 5
Änderung von Daten

§ 19
Änderung der Anschrift

(1) Die Personalausweisbehörde ändert die Anschrift auf dem Personalausweis, indem sie einen Aufkleber mit der neuen Anschrift und der Personalausweisnummer nach dem Muster in Anhang 1 anfertigt.

(2) Die Personalausweisbehörde ändert die auf dem elektronischen Speicher- und Verarbeitungsmedium gespeicherte Anschrift.

(3) Für die Änderung der Daten nach Absatz 2 sind zertifizierte Geräte mit hoheitlichem Berechtigungszertifikat zu verwenden.

§ 20
Neusetzung und Änderung der Geheimnummer

(1) Kennt der Ausweisinhaber die ursprüngliche Geheimnummer nicht, kann die Personalausweisbehörde die Neusetzung der Geheimnummer durch den Ausweisinhaber einleiten. Die Personalausweisbehörde hat zuvor die Identität des Ausweisinhabers zu überprüfen. Durch technische und organisatorische Maßnahmen hat die Personalausweisbehörde sicherzustellen, dass niemand außer dem Ausweisinhaber Kenntnis von der Geheimnummer erlangt.

(2) Der Ausweisinhaber kann die Geheimnummer durch Eingabe der bisherigen Geheimnummer und zweimalige Eingabe der neuen Geheimnummer ändern.

(3) Für die Änderung der Daten nach Absatz 1 Satz 1 sind zertifizierte Geräte mit hoheitlichem Berechtigungszertifikat zu verwenden.

§ 21
Mehrfache Fehleingabe der Geheimnummer

(1) Wurde die Geheimnummer zwei Mal falsch eingegeben, kann durch vorherige Eingabe der Zugangsnummer ein dritter Eingabeversuch freigeben werden.

(2) Wurde die Geheimnummer drei Mal falsch eingegeben, kann der elektronische Identitätsnachweis nur genutzt werden, wenn die Entsperrnummer eingegeben wird und diese nicht bereits zehn Mal benutzt wurde. Eine Verwendung der Entsperrnummer ist nach zehnmaliger Nutzung nicht mehr möglich. Sofern die Geheimnummer nach dreimaliger Falscheingabe gesperrt wurde, kann die Neusetzung der Geheimnummer ausschließlich in der Personalausweisbehörde erfolgen.

Kapitel 6
Nutzung des elektronischen Identitätsnachweises

§ 22
Nachträgliches Aus- und Einschalten

(1) Bevor die ausstellende oder zuständige Personalausweisbehörde einen eingeschalteten elektronischen Identitätsnachweis nach § 10 Absatz 3 Satz 2 des Personalausweisgesetzes ausschaltet, prüft sie die Identität des Ausweisinhabers. Die Personalausweisbehörde speichert die Tatsache der Ausschaltung im Personalausweisregister. Handelt die zuständige Personalausweisbehörde, informiert sie die ausstellende Personalausweisbehörde über die Ausschaltung. In diesem Fall speichert die ausstellende Personalausweisbehörde die Tatsache der Ausschaltung im Personalausweisregister.

(2) Bevor die ausstellende oder zuständige Personalausweisbehörde einen ausgeschalteten elektronischen Identitätsnachweis nach § 10 Absatz 3 Satz 1 des Personalausweisgesetzes einschaltet, prüft sie die Identität des Ausweisinhabers. Die Personalausweisbehörde löscht die Tatsache der Ausschaltung im Personalausweisregister. Handelt die zuständige Personalausweisbehörde findet Absatz 1 Satz 3 und 4 entsprechende Anwendung. Die Personalausweisbehörde initiiert bei jeder nachträglichen Einschaltung die Neusetzung der Geheimnummer durch den Ausweisinhaber und teilt ihm auf Wunsch das Sperrkennwort aus dem Personalausweisregister mit.

(3) Für das nachträgliche Ein- und Ausschalten des elektronischen Identitätsnachweises nach den Absätzen 1 und 2 sind zertifizierte Geräte mit hoheitlichem Berechtigungszertifikat zu verwenden.

§ 23
Voraussetzungen für die Nutzung bei dem Ausweisinhaber

(1) Vor erstmaliger Nutzung des elektronischen Identitätsnachweises soll der Ausweisinhaber die Geheimnummer einmalig durch Eingabe der im Brief übersandten ursprünglichen Geheimnummer neu setzen.

(2) Der Ausweisinhaber soll sicherstellen, dass insbesondere folgende Komponenten bei der Nutzung des elektronischen Identitätsnachweises eingesetzt werden:

1. informationstechnische Systeme mit geeigneten Abwehrmaßnahmen gegen Sicherheitslücken nach dem Stand der Technik;
2. Lesegeräte, die durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert worden sind;
3. Software zur Nutzung des elektronischen Identitätsnachweises, die durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert worden ist.

Kapitel 7
Sperrung und Entsperrung des elektronischen Identitätsnachweises

§ 24
Referenzliste; allgemeine Sperrliste

(1) Der Sperrlistenbetreiber führt eine Referenzliste der Sperrsummen, der Sperrschlüssel und des Datums der Übermittlung dieser Daten vom Ausweishersteller. Die Referenzliste enthält die in Satz 1 genannten Daten aller Personalausweise. Sie darf ausschließlich für die Ermittlung des Sperrschlüssels zu einer übermittelten Sperrsumme verwendet werden.

(2) Der Sperrlistenbetreiber führt eine allgemeine Sperrliste. Sie enthält allgemeine Sperrmerkmale gesperrter elektronischer Identitätsnachweise und wird Berechtigungszertifikateanbietern auf Anfrage zur Umrechnung in dienstespezifische Sperrlisten bereitgestellt.

§ 25
Sperrung des elektronischen Identitätsnachweises

(1) Kommt ein Personalausweis abhanden, hat der Ausweisinhaber den elektronischen Identitätsnachweis über die zuständige oder ausstellende Personalausweisbehörde oder den Sperrnotruf, der auch vom Ausland aus erreichbar ist, unverzüglich sperren zu lassen. Die Stelle, über die der Ausweisinhaber den elektronischen Identitätsnachweis nach Satz 1 sperren lässt, hat den Ausweisinhaber vor der Sperrung zu identifizieren. Die Sperrung kann unter Angabe des Sperrkennworts, des Familiennamens, der Vornamen und des Tages der Geburt, gegenüber der zuständigen oder ausstellenden Personalausweisbehörde auch ohne Angabe des Sperrkennworts geschehen.

(2) Die Stelle, über die der Ausweisinhaber den elektronischen Identitätsnachweis nach Absatz 1 Satz 1 sperren lässt, erzeugt unverzüglich die Sperrsumme und übermittelt sie unverzüglich dem Sperrlistenbetreiber. Handelt die zuständige Personalausweisbehörde, informiert diese die ausstellende Personalausweisbehörde über den Sperrantrag. Die ausstellende Personalausweisbehörde dokumentiert die Tatsache der Sperrung im Personalausweisregister.

(3) Der Sperrlistenbetreiber hat den Eintrag des allgemeinen Sperrmerkmals in die Sperrliste unverzüglich zu bestätigen und an den Ausweisinhaber weiterzuleiten. Lässt der Ausweisinhaber den elektronischen Identitätsnachweis über die zuständige oder ausstellende Personalausweisbehörde sperren, hat die Bestätigung gegenüber der ausstellenden Personalausweisbehörde zu erfolgen. Lässt der Ausweisinhaber den elektronischen Identitätsnachweis über den Sperrnotruf sperren, hat die Bestätigung gegenüber dem Sperrnotruf zu erfolgen.

§ 26
Entsperrung des elektronischen Identitätsnachweises

(1) Der Ausweisinhaber kann die Entsperrung eines gesperrten elektronischen Identitätsnachweises bei der ausstellenden oder zuständigen Personalausweisbehörde beantragen. Die Entsperrung erfolgt nach der Identifizierung des Ausweisinhabers. Der Ausweisinhaber muss hierzu persönlich erscheinen.

(2) Handelt die zuständige Personalausweisbehörde informiert sie die ausstellende Personalausweisbehörde über den Entsperrantrag. Diese übermittelt dem Sperrlistenbetreiber die Sperrsumme und löscht im Personalausweisregister die Eintragung des Personalausweises in die Sperrliste.

(3) Die Löschung des allgemeinen Sperrmerkmals aus der Sperrliste ist der ausstellenden Personalausweisbehörde vom Sperrlistenbetreiber zu bestätigen. Die ausstellende Personalausweisbehörde leitet die Bestätigung an den Ausweisinhaber weiter.

§ 27
Auskunft über Sperrung

Der Sperrlistenbetreiber hat die technischen und organisatorischen Vorkehrungen dafür zu treffen, dass der Ausweisinhaber Auskunft darüber erhält, ob der elektronische Identitätsnachweis in der allgemeinen Sperrliste eingetragen ist. Die gleiche Auskunft ist der Personalausweisbehörde über elektronische Identitätsnachweise von Personalausweisen zu erteilen, die von ihr ausgestellt worden sind.

Kapitel 8
Beantragung von Berechtigungen

§ 28
Antrag

(1) Um das Vorliegen der Voraussetzungen des § 21 Absatz 2 Satz 1 des Personalausweisgesetzes überprüfen zu können, muss ein Antrag nach § 21 Absatz 1 Satz 1 des Personalausweisgesetzes enthalten:

1. Angaben zur Identitätsfeststellung von juristischen und natürlichen Personen; bei natürlichen Personen sind dies insbesondere der Familienname, die Vornamen, der Tag und der Ort der Geburt sowie die Anschrift der Hauptwohnung; bei juristischen Personen sind diese insbesondere der Name, die Anschrift des Sitzes, die Rechtsform und die Bevollmächtigten; außerdem ist in diesem Fall eine Kopie des Handelsregisterauszugs oder der Errichtungsurkunde beizulegen;
2. Kontaktdaten, insbesondere die Telefon- und Faxnummer sowie die E-Mail-Adresse;
3. Angaben zu antragstellenden Personen mit Wohnung oder Sitz außerhalb Deutschlands, soweit zur eindeutigen länderspezifischen Identifizierung erforderlich, einschließlich einer ladungsfähigen Anschrift; soweit eine Niederlassung in Deutschland besteht, sind auch deren Angaben nach den Nummern 1 und 2 aufzunehmen;
4. eine Beschreibung des Diensteanbieters und seiner Tätigkeitsfelder sowie die Angabe der Unternehmenswebsite, soweit vorhanden;
5. eine Beschreibung des Diensteangebots für das das Berechtigungszertifikat gelten soll, einschließlich einer Angabe der Internetseite auf der das Berechtigungszertifikat genutzt wird oder des Standortes bei Automaten und eines Verweises auf die für das Angebot geltende Datenschutzerklärung;
6. eine hinreichende Beschreibung des Zwecks der Datenerhebung, für den die Berechtigung ausgestellt werden soll;
7. eine Angabe der Datenkategorien nach § 18 Absatz 3 des Personalausweisgesetzes, auf die die antragstellende Person zugreifen möchte; hierbei ist für jede Datenkategorie zu begründen, warum es für den dargelegten Zweck erforderlich ist, die Daten zu erheben;
8. Angaben zum oder zur betrieblichen oder behördlichen Datenschutzbeauftragten nach § 4f des Bundesdatenschutzgesetzes (Name, Anschrift, Telefonnummer, E-Mail-Adresse) und zur zuständigen Datenschutzaufsichtsbehörde (Name, Sitz, Anschrift, Telefonnummer, E-Mail-Adresse);
9. die Angabe, ob die antragstellende Person sich eines Auftragnehmers nach § 11 des Bundesdatenschutzgesetzes zur Durchführung des elektronischen Identitätsnachweises bedienen wird und gegebenenfalls die Angaben nach Nummer 1 für diesen Auftragnehmer; ist diese Angabe zum Zeitpunkt des Antrages noch nicht bekannt, so ist sie sobald bekannt unverzüglich nachzuliefern.

(2) Der Antrag ist von der antragstellenden Person zu unterschreiben oder mit einer qualifizierten elektronischen Signatur zu versehen. Die antragstellende Person ist zu identifizieren durch:

1. persönliches Erscheinen und Vorlage eines amtlichen Lichtbildausweises der antragstellenden Person bei juristischen Personen einer vertretungsberechtigten Person bei der Vergabestelle für Berechtigungszertifikate oder geeigneten Dritten,
2. eine qualifizierte elektronische Signatur oder
3. den elektronischen Identitätsnachweis.

Die Vergabestelle für Berechtigungszertifikate bestimmt, welche der genannten Arten des Identitätsnachweises genutzt werden können.

§ 29
Anforderungen an Datenschutz und -sicherheit

(1) Anforderungen im Sinne des § 21 Absatz 2 Satz 1 Nummer 4 des Personalausweisgesetzes liegen insbesondere nicht vor, wenn

1. der Zweck der Datenerhebung ausschließlich in der Auslesung oder Bereitstellung personenbezogener Daten aus dem Personalausweis für den Ausweisinhaber oder Dritte besteht,
2. der Staat des Wohnsitzes oder des Sitzes der antragstellenden Person kein angemessenes Datenschutzniveau gewährleistet entsprechend der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*ABl. L 281 vom 23.11.1995, S. 31)*,
3. der elektronische Identitätsnachweis für den Diensteanbieter durch einen Auftragnehmer nach § 11 des Bundesdatenschutzgesetzes durchgeführt wird und hierbei kein wirksames Auftragsverhältnis nach § 11 des Bundesdatenschutzgesetzes zwischen dem Diensteanbieter und dem Auftragnehmer besteht,
4. der Diensteanbieter einen Auftragnehmer nach § 11 des Bundesdatenschutzgesetzes gewählt hat, der die technischen und organisatorischen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik für die sichere Bereitstellung des elektronischen Identitätsnachweises nicht erfüllt.

(2) Die Anforderungen an die Datensicherheit im Sinne des § 21 Absatz 2 Satz 1 Nummer 4 des Personalausweisgesetzes sind durch die Diensteanbieter nach dem Stand der Technik zu erfüllen. Art und Umfang der einzusetzenden Systemkomponenten legt die Vergabestelle für Berechtigungszertifikate in der Berechtigung fest. Die Vergabestelle für Berechtigungszertifikate legt in Richtlinien die weiteren technischen und organisatorischen Anforderungen fest, die ein Diensteanbieter zu erfüllen hat, um für die Nutzung von Berechtigungszertifikaten zugelassen zu werden. Die Richtlinien gelten in der jeweils im elektronischen Bundesanzeiger veröffentlichten Fassung.

(3) Vor Erteilung einer Berechtigung für einen nicht-öffentlichen Diensteanbieter kann die Vergabestelle für Berechtigungszertifikate eine Stellungnahme der zuständigen Datenschutzaufsichtsbehörde einholen, ob dort Umstände bekannt sind, aus denen sich Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung ergeben.

§ 30
Öffentliche Liste der Berechtigungen

Die Vergabestelle für Berechtigungszertifikate veröffentlicht eine Liste aller erteilten gültigen Berechtigungen. Dabei sind die Angaben nach § 18 Absatz 4 Satz 2 Nummer 1 bis 4 des Personalausweisgesetzes und die Gültigkeitsdauer der Berechtigung zu veröffentlichen. Die Daten dürfen ausschließlich für Zwecke des elektronischen Identitätsnachweises verwendet werden.

Kapitel 9
Ausgabe von Berechtigungszertifikaten

§ 31
Anzeige der Ausgabe von Berechtigungszertifikaten

Berechtigungszertifikateanbieter dürfen Berechtigungszertifikate für den elektronischen Identitätsnachweis bereitstellen, wenn sie vor Aufnahme dieser Tätigkeit

1. der zuständigen Behörde nach § 3 des Signaturgesetzes die Aufnahme des Betriebs eines Zertifizierungsdienstes nach § 4 Absatz 3 des Signaturgesetzes angezeigt haben oder nach § 15 des Signaturgesetzes akkreditiert worden sind,
2. der Vergabestelle für Berechtigungszertifikate die Anzeige nach Nummer 1 vorgelegt und ihr gegenüber die in § 28 Absatz 1 Nummer 1 bis 3, 8 und 9 sowie Absatz 2 aufgeführten Angaben gemacht haben.

§ 32
Beachtung der Anforderungen des Inhabers der Wurzelzertifikate

Das Bundesamt für Sicherheit in der Informationstechnik ist Inhaber der Wurzelzertifikate für Berechtigungszertifikate zum elektronischen Identitätsnachweis. Die Zertifikatsrichtlinien des Bundesamtes für Sicherheit in der Informationstechnik für die technischen und organisatorischen Voraussetzungen für die Ausstellung von Berechtigungszertifikaten sind vom Berechtigungszertifikateanbieter einzuhalten. Die Richtlinien gelten in der jeweils im elektronischen Bundesanzeiger veröffentlichten Fassung.

§ 33
Beachtung der Berechtigung durch den Berechtigungszertifikateanbieter

Vor der Ausgabe von Berechtigungszertifikaten hat der Berechtigungszertifikateanbieter zu überprüfen, ob eine Berechtigung der Vergabestelle für Berechtigungszertifikate vorliegt. Er hat Auflagen, Beschränkungen und Nebenbestimmungen der Berechtigung zu beachten. Bei Zweifeln über den Inhaber, die Gültigkeit oder den Umfang einer Berechtigung hat er vor der Ausstellung von Berechtigungszertifikaten die Vergabestelle für Berechtigungszertifikate zu informieren. Wird ein Berechtigungszertifikat widerrufen oder zurückgenommen, informiert die Vergabestelle für Berechtigungszertifikate den vom Diensteanbieter beauftragten Berechtigungszertifikateanbieter.

§ 34
Gültigkeitsdauer von Berechtigungszertifikaten

Die Vergabestelle für Berechtigungszertifikate legt mit Erteilung der Berechtigung die Gültigkeitsdauer der Berechtigungszertifikate fest. Das Bundesamt für Sicherheit in der Informationstechnik legt angemessene Höchstgrenzen für die Gültigkeitsdauer von Berechtigungszertifikaten fest. Es hat sich dabei am Risiko des Einsatzumfeldes und an den beantragten Datenkategorien zu orientieren.

§ 35
Speicherung, Abruf und Verwendung von Daten durch Berechtigungszertifikateanbieter

(1) Berechtigungszertifikateanbieter sind verpflichtet, sich zur Erzeugung von Listen, die Sperrmerkmale im Sinne des § 2 Absatz 7 des Personalausweisgesetzes enthalten, der jeweils aktuellen Liste der allgemeinen Sperrmerkmale nach § 1 Absatz 4 zu bedienen. Dazu rufen sie regelmäßig die Liste der allgemeinen Sperrmerkmale ab, rechnen die allgemeinen Sperrmerkmale in Sperrmerkmale um und stellen sie für die Diensteanbieter bereit.

(2) Berechtigungszertifikateanbieter dürfen die allgemeinen Sperrlisten, die vom Sperrlistenbetreiber bereitgestellt worden sind, nur bis zum Abruf einer neueren Sperrliste speichern und verwenden.

(3) Die Daten aus der allgemeinen Sperrliste dürfen nur dazu verwendet werden, dienstespezifische Sperrlisten mit Sperrmerkmalen zu erstellen.

§ 36
Ausgabe von hoheitlichen Berechtigungszertifikaten

(1) Hoheitliche Berechtigungszertifikate nach § 2 Absatz 4 Satz 3 des Personalausweisgesetzes dürfen ausschließlich an die zur Identitätsfeststellung berechtigten Behörden ausgegeben werden.

(2) Das Bundesministerium des Innern bestimmt, welche Stellen hoheitliche Berechtigungszertifikate an welche zur Identitätsfeststellung berechtigten Behörden ausgeben dürfen und veröffentlicht dies im elektronischen Bundesanzeiger.

(3) Die Gültigkeitsdauer hoheitlicher Berechtigungszertifikate wird nach den Vorgaben des § 34 Satz 3 vom Bundesamt für Sicherheit in der Informationstechnik festgelegt.

(4) Zur Ausgabe berechtigte Stellen dokumentieren Empfänger, zugrundeliegende Berechtigung sowie das Datum und die Uhrzeit der Ausgabe von Berechtigungszertifikaten.

Kapitel 10
Schlussvorschriften

§ 37
Übergangsregelungen

(1) Vordrucke für vorläufige Personalausweise, die der Anlage 2 der bis zum 31. Oktober 2010 geltenden Verordnung zur Bestimmung der Muster der Personalausweise der Bundesrepublik Deutschland entsprechen, können bis zum 31. Oktober 2011 weiterverwendet werden.

(2) Signaturkarten, die der Ausweishersteller zur Absicherung des elektronischen Antragsprozesses der Ausweisbehörde vor dem 1. November 2010 ausgestellt hat, behalten bis zum Ablauf der Gültigkeitsdauer ihre Geltung.

§ 38
Inkrafttreten

Diese Verordnung tritt mit Wirkung vom 1. November 2010 in Kraft.

Der Bundesrat hat zugestimmt.

Berlin, den 1. November 2010

Der Bundesminister des Innern

Thomas de Maizière

Anhang 1

Muster des Personalausweises

Vorderseite

Rückseite

Muster des Aufklebers zur Anschriftenänderung

Anhang 2

Muster des vorläufigen Personalausweises

Vorderseite

Rückseite

Anhang 3

Formale Anforderungen an die Einträge im Personalausweis

Abschnitt 1

Datenfelder	Anzahl der zur Verfügung stehenden Zeichen	
	Schriftgröße 1 (2 mm)[1]	**Schriftgröße 2 (1,3 mm)**
Familienname und Geburtsname[2]	26 Zeichen pro Zeile; 2 Zeilen (insgesamt 52 Zeichen)	40 Zeichen pro Zeile; 3 Zeilen (insgesamt 120 Zeichen)
Vornamen	26 Zeichen pro Zeile; 1 Zeile (insgesamt 26 Zeichen)	40 Zeichen pro Zeile; 2 Zeilen (insgesamt 80 Zeichen)
Tag der Geburt	10 Zeichen pro Zeile; 1 Zeile (insgesamt 10 Zeichen)	-[3]
Ort der Geburt	26 Zeichen pro Zeile; 1 Zeile (insgesamt 26 Zeichen)	40 Zeichen pro Zeile; 2 Zeilen (insgesamt 80 Zeichen)
Staatsangehörigkeit	7 Zeichen pro Zeile; 1 Zeile (insgesamt 7 Zeichen)	-
Letzter Tag der Gültigkeitsdauer	10 Zeichen pro Zeile; 1 Zeile (insgesamt 10 Zeichen)	-
Anschrift	25 Zeichen pro Zeile; 2 Zeilen (insgesamt 50 Zeichen)	-
Straße und Hausnummer	25 Zeichen pro Zeile; 2 Zeilen (insgesamt 50 Zeichen	-
Größe	3 Zeichen pro Zeile; 1 Zeile (insgesamt 3 Zeichen)	-

[1] Soweit nicht die max. Anzahl der zur Verfügung stehenden Zeichen ausgenutzt wird, werden die Daten in der Schriftgröße 1 und in einer Zeile eingetragen. Die Datenfelder „Familienname und Geburtsname“, „Wohnort“, „Straße“, „Ordens- und Künstlername“ und „ausstellende Behörde“ können auch in der Schriftgröße 1 zweizeilig dargestellt werden. Falls erforderlich, können die Daten in den Feldern „Familienname und Geburtsname“, „Vornamen“, „Ort der Geburt“ und „ausstellende Behörde“ auch in der Schriftgröße 2 mit jeweils einer zusätzlichen Zeile eingetragen werden.

[2] Wenn der Familienname vom Geburtsnamen abweicht, kommt diesem mindestens eine vollständige Zeile zu. Am Beginn dieser Zeile werden fünf Zeichen durch die Zeichenfolge „GEB. " belegt.

[3] Für bestimmte Datenfelder ist die Schriftgröße 2 nicht vorgesehen.

Datenfelder	**Anzahl der zur Verfügung stehenden Zeichen**	
	Schriftgröße 1 (2 mm)[4]	**Schriftgröße 2 (1,3 mm)**
Farbe der Augen	19 Zeichen pro Zeile; 1 Zeile (insgesamt 19 Zeichen)	-
Ordens- und Künstlername	20 Zeichen pro Zeile; 1 Zeilen (insgesamt 20 Zeichen)	30 Zeichen pro Zeile; 2 Zeilen (insgesamt 60 Zeichen -
Ausstellende Behörde	19 Zeichen pro Zeile; 2 Zeilen (insgesamt 38 Zeichen)	28 Zeichen pro Zeile; 3 Zeilen (insgesamt 84 Zeichen)
Tag der Ausstellung	8 Zeichen pro Zeile; 1 Zeilen (insgesamt 8 Zeichen)	-

Datenfelder **- der Aufkleber für Anschriftänderungen**	**Anzahl der zur Verfügung stehenden Zeichen**
	Schriftgröße 3 (1,5 mm)[5]
Anschrift	25 Zeichen pro Zeile; 4 Zeilen (insgesamt 100 Zeichen)
Seriennummer	9 Zeichen pro Zeile; 1 Zeile (insgesamt 9 Zeichen)

[4] Soweit nicht die maximale Anzahl der zur Verfügung stehenden Zeichen ausgenutzt wird, werden die Daten in der Schriftgröße 1 und in einer Zeile eingetragen. Die Datenfelder „Familienname und Geburtsname“, „Wohnort“, „Straße“, „Ordens- und Künstlername“ und „ausstellende Behörde“ können auch in der Schriftgröße 1 zweizeilig dargestellt werden. Falls erforderlich, können die Daten in den Feldern „Familienname und Geburtsname“, „Vorname“, „Ort der Geburt“ und „ausstellende Behörde“ auch in der Schriftgröße 2 mit jeweils einer zusätzlichen Zeile dargestellt werden.

[5] Für die Tintenstrahldrucker in den Personalausweisbehörden sind folgende Einstellungen erforderlich: Für die Anschrift ist die Schriftart Arial Fett im Schriftgrad 6 Punkt zu verwenden und für die Seriennummer die Schriftart Arial im Schriftgrad 6 Punkt.

Abschnitt 2

Musterfoto

Qualitativ hochwertige Fotos sind die Grundlage einer einwandfreien Wiedergabe des Bildes und Voraussetzung für die Anwendung der Gesichtsbiometrie in Personalausweisen. Dieser Foto-Mustertafel sind die Qualitätsmerkmale zu entnehmen, die die Eignung der Fotos für den vorgesehenen Einsatz in Personalausweisen gewährleisten. Es ist dringend erforderlich, die hier beschriebenen Anforderungen zu beachten, da sonst eine biometrische Erkennung der antragstellenden Person sowie die einwandfreie Wiedergabe des Bildes im Dokument nicht gewährleistet sind. Der antragstellenden Person ist grundsätzlich ohne Kopfbedeckung abzubilden. Die Ausweisbehörde kann vom Gebot der fehlenden Kopfbedeckung insbesondere aus religiösen Gründen, von den übrigen Anforderungen aus medizinischen Gründen, die nicht nur vorübergehender Art sind, Ausnahmen zulassen. Auf den Fotos sind keine Uniformteile abzubilden.

Format

Das Foto muss die Gesichtszüge der Person von der Kinnspitze bis zum oberen Kopfende, sowie die linke und rechte Gesichtshälfte deutlich zeigen. Die Gesichtshöhe muss 70 bis 80 Prozent des Fotos einnehmen. Dies entspricht einer Höhe von 32 bis 36 Millimeter von der Kinnspitze bis zum oberen Kopfende. Dabei ist das obere Kopfende unter Vernachlässigung der Frisur anzunehmen. Wegen des häufig nicht eindeutig zu bestimmenden oberen Kopfendes sind Lichtbilder jedoch erst dann abzulehnen, wenn die Gesichtshöhe 27 Millimeter unterschreitet oder 40 Millimeter überschreitet. Bei volumenreichem Haar sollte darauf geachtet werden, dass der Kopf (einschließlich Frisur) möglichst vollständig abgebildet ist, ohne aber die Gesichtsgröße zu verkleinern. Das Gesicht muss zentriert auf dem Foto platziert sein.

Schärfe und Kontrast

Das Gesicht muss in allen Bereichen scharf abgebildet, kontrastreich und klar sein.

Ausleuchtung

Das Gesicht muss gleichmäßig ausgeleuchtet werden. Reflexionen oder Schatten im Gesicht sowie rote Augen sind zu vermeiden.

Hintergrund

Der Hintergrund muss einfarbig hell sein (idealerweise neutral grau) und einen Kontrast zum Gesicht und zu den Haaren aufweisen. Bei hellen Haaren eignet sich ein mittelgrauer Hintergrund, bei dunklen Haaren ein hellgrauer. Der Hintergrund darf kein Muster aufweisen. Das Foto darf ausschließlich die zu fotografierende Person zeigen (keine weiteren Personen oder Gegenstände im Bild). Auf dem Hintergrund dürfen keine Schatten entstehen.

Fotoqualität

Das Foto sollte (insbesondere bei der Aufnahme mit einer Digitalkamera) auf hochwertigem Papier mit einer Druckauflösung von mindestens 236 Punkte pro Zentimeter (600 dots per inch) vorliegen. Das Foto muss farbneutral sein und die Hauttöne natürlich wiedergeben. Das Foto darf keine Knicke oder Verunreinigungen aufweisen. Das Foto kann in Schwarzweiß oder Farbe vorliegen.

Kopfposition und Gesichtsausdruck

Eine Darstellung der Person mit geneigtem oder gedrehtem Kopf (zum Beispiel Halbprofil) ist nicht zulässig. Die Person muss mit neutralem Gesichtsausdruck und geschlossenem Mund gerade in die Kamera blicken.

Augen und Blickrichtung

Die Person muss auf dem Foto direkt in die Kamera blicken. Die Augen müssen geöffnet und deutlich sichtbar sein und dürfen nicht durch Haare oder Brillengestelle verdeckt werden.

Brillenträger

Die Augen müssen klar und deutlich erkennbar sein (Reflexionen auf den Brillengläsern, getönte Gläser oder Sonnenbrillen sind nicht zulässig). Der Rand der Gläser oder das Gestell dürfen nicht die Augen verdecken.

Kopfbedeckung

Kopfbedeckungen sind grundsätzlich nicht erlaubt. Ausnahmen sind insbesondere aus religiösen Gründen zulässig. In diesem Fall gilt: das Gesicht muss von der unteren Kinnkante bis zur Stirn erkennbar sein. Es dürfen keine Schatten auf dem Gesicht entstehen.

Kinder

Bei Kindern bis zum vollendeten zehnten Lebensjahr sind folgende Abweichungen bei der Gesichtshöhe und im Augenbereich zulässig: Die Gesichtshöhe bei Kindern muss 50 bis 80 Prozent des Fotos einnehmen. Dies entspricht einer Höhe von 22 bis 36 Millimeter von der Kinnspitze bis zum oberen Kopfende. Dabei ist das obere Kopfende unter Vernachlässigung der Frisur anzunehmen. Wegen des häufig nicht eindeutig zu bestimmenden oberen Kopfendes sind Fotos jedoch erst dann abzulehnen, wenn die

Gesichtshöhe 17 Millimeter unterschreitet oder 40 Millimeter überschreitet. Bei Säuglingen und Kleinkindern gelten zusätzlich die nachfolgend beschriebenen Abweichungen.

Säuglinge und Kleinkinder

Bei Säuglingen und Kleinkindern bis zum vollendeten sechsten Lebensjahr sind zusätzlich zu den unter der Überschrift „Kinder" dargestellten Ausnahmen Abweichungen in der Kopfhaltung (nicht von der Frontalaufnahme!), im Gesichtsausdruck, hinsichtlich Augen und Blickrichtung sowie hinsichtlich der Zentrierung auf dem Foto zulässig.

Anhang 4

Übersicht über die Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

1. BSI: Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen
2. BSI: Technische Richtlinie TR-03104, Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für hoheitliche Dokumente (TR PDÜ hD)
3. BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI) [Fortgeschrittene Sicherheitsmechanismen für maschinenlesbare Reisedokumente]
4. BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC) [Elliptische-Kurven-Kryptographie]
5. BSI: Technische Richtlinie TR-03112, eCard-API-Framework
6. BSI: Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung – Hoheitliche Ausweisdokumente
7. BSI: Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit
8. BSI: Technische Richtlinie TR-03119, Anforderungen an Kartenleser mit -Unterstützung des Personalausweises
9. BSI: Technische Richtlinie TR-03121, Biometrics for Public Sector Applications [Technische Richtlinie für Biometrie in hoheitlichen Anwendungen]
10. BSI: Technische Richtlinie TR-03123, XML-Datenaustauschformat für hoheitliche Dokumente (TR XhD)
11. BSI: Technische Richtlinie TR-03127, Architektur Elektronischer Personalausweis
12. BSI: Technische Richtlinie TR-03128, Public Key Infrastrukturen für den elektronischen Personalausweis
13. BSI: Technische Richtlinie TR-03129, Communication Protocols for Extended Access Control [Kommunikationsprotokolle für die erweiterte Zugriffskontrolle]
14. BSI: Technische Richtlinie TR-03130, eID-Server
15. BSI: Technische Richtlinie TR-03131, EAC-Box Architecture and Interfaces [EAC-Box Architektur und Schnittstellen]
16. BSI: Technische Richtlinie TR-03132, Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente (TR SiSKo hD)
17. BSI: Common Criteria Protection Profile Electronic Identity Card, BSI-CC-PP-0061 [Gemeinsame Kriterien – Schutzprofil Elektronische Identitätskarte]
18. BSI: Common Criteria Protection Profile for Inspection Systems (IS), BSI-CC-PP-0064 [Gemeinsame Kriterien – Schutzprofil für Inspektionssysteme]

Anhang 5

Übersicht über die zu zertifizierenden Systemkomponenten

Nr.	Bezeichnung der Systemkomponente	Verpflichtung / Option
1	Elektronisches Speicher- und Verarbeitungsmedium auf der Ausweiskarte (Hard- und Software)	Verpflichtung für den Ausweishersteller
2	Fingerabdruckleser	Verpflichtung für die Anbieter dieser Geräte Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden
3	Software zur Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke	Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden
4	System zur sicheren Übermittlung des Lichtbilds von Dritten an die Personalausweisbehörde	Verpflichtung für die Personalausweisbehörden, welche das Lichtbild gemäß § 7 Absatz 1 Satz 2 Nummer 1 von Dritten erhalten
5	Erfassungsstation zur Fertigung des Lichtbildes	Verpflichtung für die Personalausweisbehörden, die das Lichtbild gemäß § 7 Absatz 1 Satz 2 Nummer 2 selbst fertigen
6	Modul für die Datenübermittlung von den Personalausweisbehörde an den Ausweishersteller	Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden
7	Modul zur Sicherung der Authentizität und Vertraulichkeit der Antragsdaten	Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden
8	Änderungs- und Visualisierungmodul für den Änderungs- und Visualisierungsdienst in den Personalausweisbehörden	Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden
9	Kartenlesegeräte für die Nutzung im Rahmen des § 18 des Personalausweisgesetzes	Optionale Durchführung durch den Anbieter dieser Geräte. Empfehlung des Einsatzes zertifizierter Geräte an den Ausweisinhaber
10	Bürgerclient	Optionale Durchführung durch den Anbieter dieser Software. Empfehlung des Einsatzes zertifizierter Software an den Ausweisinhaber
11	Hard- und Software zur Durchführung des elektronischen Identitätsnachweises bei den Diensteanbietern oder ihrer Auftragnehmer (eID-Server)	Verpflichtung für den Diensteanbieter oder dessen Auftragnehmer

Begründung

A. Allgemeiner Teil

Der vorliegende Verordnungsentwurf nimmt die in § 34 des Personalausweisgesetzes erteilte Verordnungsermächtigung auf und gestaltet den rechtlichen Rahmen zur Ausgabe und Nutzung des Personalausweises und des elektronischen Identitätsnachweises aus.

Der Personalausweis dient als hoheitliches Dokument der sicheren Identifizierung des Inhabers. Darüber hinaus kann er auch als Reisedokument genutzt werden. Mit den im elektronischen Speicher- und Verarbeitungsmedium gespeicherten biometrischen Merkmalen (Gesichtsbild und ggf. Fingerabdrücke) wird die Sicherheit der angestrebten Identifizierung des Inhabers erhöht und eine Vereinfachung im grenzüberschreitenden Verkehr herbeigeführt.

Der elektronische Identitätsnachweis im Personalausweis wird die zuverlässige gegenseitige Identifizierung im elektronischen Rechts- und Geschäftsverkehr, sowohl in Online-Anwendungen als auch in lokalen Verarbeitungsprozessen wie etwa an Automaten ermöglichen. Dadurch besteht die Möglichkeit des zuverlässigen Nachweises der Identität in der elektronischen Kommunikation – sowohl im E-Government als auch im E-Business.

Der elektronische Identitätsnachweis ist so ausgestaltet, dass er den Diensteanbietern auf hohem sicherheitstechnischem Niveau die Überprüfung der Identität der Ausweisinhaber ermöglicht. Gleichzeitig sichert das Konzept durch ein Zusammenspiel rechtlicher Vorgaben, technischer Vorkehrungen und organisatorischer Maßnahmen die informationelle Selbstbestimmung der Bürgerinnen und Bürger, indem eine von einem bestimmten Diensteanbieter gewünschte Datenübermittlung transparent gemacht wird und nur nach ausdrücklicher Freigabe durch den Ausweisinhaber erfolgt.

Im Rahmen der Ausstellung der Berechtigungszertifikate wird neben der Identität des Diensteanbieters auch die Erforderlichkeit der Datenübermittlung für den genannten Zweck geprüft. Ein Diensteanbieter kann im Zuge des Identifizierungsprozesses daher technisch nur die Daten abfragen, die für die Erbringung seines Dienstes erforderlich sind. Durch die gegenseitige Identifizierung von Diensteanbieter und Ausweisinhaber trägt dieses Verfahren zur Bekämpfung der stark zunehmenden Fälle des Identitätsdiebstahls durch sogenanntes Phishing bei und entspricht gleichzeitig dem Verbraucherschutz, indem eine übermäßige Erhebung personenbezogener Daten aus dem Personalausweis unterbunden wird. Darüber hinaus ermöglicht das System der nur kurz gültigen Berechtigungszertifikate eine zeitliche Beschränkung der Berechtigung zur Datenanfrage und eine kurzfristige Aufhebung der Berechtigung ohne übermäßigen Verwaltungsaufwand, falls ein Diensteanbieter diese Funktion missbraucht.

Die Nutzung des elektronischen Identitätsnachweises wird Ausweisinhabern nicht aufgezwungen. Die Bürgerinnen und Bürger können jederzeit seine Ausschaltung verlangen. Die Funktion kann grundsätzlich erst mit Erreichen der Ausweispflicht aktiviert werden. Risiken - etwa durch unsachgemäße Handhabung der Geheimnummer - für Ausweisinhaber, die noch nicht 16 Jahre alt sind, sind damit ausgeschlossen. Darüber hinaus liegt es in der freien Entscheidung des Ausweisinhabers, wann und gegenüber welchem Diensteanbieter er den elektronischen Identitätsnachweis nutzt.

Durch den elektronischen Identitätsnachweis werden die Anforderungen des informationellen Selbstbestimmungsrechts umgesetzt. Der Ausweisinhaber behält zu jedem Zeitpunkt die Kontrolle über seine Daten und bestimmt selbst über deren Weitergabe. Er kann den elektronischen Identitätsnachweis sowohl vollständig ausschalten als auch in jedem einzelnen Fall die Übertragung seiner Daten kontrollieren und verhindern. Die Begrenzung der Berechtigungszertifikate beschränkt bereits auf technischem Wege die Menge der ab-gerufenen Daten auf das Erforderliche.

Die Diensteanbieter stehen unter der Aufsicht der für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz zuständigen Stellen. Diese haben die Möglichkeit, die

Aufhebung der Berechtigung zu verlangen, wenn Tatsachen die Annahme rechtfertigen, dass ein Diensteanbieter die auf Grund des Berechtigungszertifikats erhaltenen personenbe-zogenen Daten in unzulässiger Weise verarbeitet oder nutzt (§ 21 Absatz 5 Satz 3 des Personalausweisgesetzes).

Ergänzend zu dieser elektronischen Grundfunktionalität, die die Ausweisfunktion des Personalausweises der realen Welt auch für die sich ausbreitende elektronische Welt nutzbar macht, kann der Ausweis auch als Träger einer Funktion für die qualifizierte elektronische Signatur dienen und so zum universellen Werkzeug (rechts-)verbindlichen Handelns im elektronischen Umfeld werden. Die optionale Signaturfunktion schafft für die Ausweisinhaber die Voraussetzungen dafür, im elektronischen Rechtsverkehr Erklärungen abzugeben, die hinsichtlich Integrität und Authentizität dauerhaft beweisbar sind. Der elektronische Personalausweis ermöglicht diese Funktion, ohne Vorgaben für den Ausweisinhaber zu machen. Die Signaturfunktion wird dem Ausweisinhaber nur auf Antrag bei einem Berechtigungszertifikateanbieter zur Verfügung stehen. Die Zusammenarbeit der Berechtigungszertifikateanbieter mit Dritten, die Ausstellung von Zertifikaten und die Entwicklung entsprechender Geschäftsmodelle bleiben dem Markt überlassen. Es kann vollständig auf den vorhandenen Rechtsrahmen des Signaturrechts zurückgegriffen werden.

Der Entwurf ist mit dem Recht der Europäischen Union vereinbar.

Bürokratiekosten

Es werden 11 Informationspflichten für die Wirtschaft geschaffen. 4 „Informationspflichten“, die nur für den Ausweishersteller gelten, werden zwischen der Bundesrepublik Deutschland und dem Ausweishersteller vertraglich normiert. Eine weitere Informationspflicht wird mit dem Betreiber des Sperrnotrufs vertraglich vereinbart. Die Verordnung enthält darüber hinaus für die Bürgerinnen und Bürger 4 Informationspflichten. 1 bestehende Informationspflicht wird geändert, 3 werden neu eingeführt. Schließlich enthält die Verordnung 13 Informations-pflichten für die Verwaltung. 2 Pflichten bestanden bereits im Vorfeld - eine dieser Informa-tionspflichten wurde geändert, eine bleibt unverändert bestehen. 11 Informationspflichten für die Verwaltung werden neu eingeführt.

Der vorliegende Verordnungsentwurf ist zwingende Voraussetzung zur Umsetzung einer Reihe von weiteren Bürokratieabbaumaßnahmen und –synergien, so dass der Aufwuchs von neuen Informationspflichten in diesem Fall gerechtfertigt und hinnehmbar ist.

Im Folgenden sollen daher die aus den neu geschaffenen Informationspflichten zu erwartenden Synergien und Entlastungen in Teilen dargestellt werden.

Wirtschaft

Die Wirtschaft im allgemeinen und insbesondere mittelständische Unternehmen werden den Personalausweis weiterhin als Sichtausweis nutzen können und künftig zusätzlich über eine Möglichkeit zur elektronischen Identifizierung von Kunden und Geschäftspartnern verfügen, die sichere und schlankere Geschäftsprozesse ermöglicht.

Der Wirtschaft wird somit ein Instrument an die Hand gegeben, das die gewünschte Abwicklung von elektronischen Geschäftsprozessen erheblich vereinfacht. Unternehmen werden zukünftig in der Lage sein, elektronische Dienste anzubieten, die einer Identitäts-prüfung einer Bürgerin bzw. eines Bürgers bedürfen und daher bisher nicht online durchgeführt werden können. Mit der Verwendung von so genannten Berechtigungs-zertifikaten erhalten Unternehmen die Möglichkeit, auf bestimmte Daten im elektronisches Speicher- und Verarbeitungsmedium des Personalausweises zuzugreifen. Auf Basis dieses Zertifikats kann sich auch die Bürgerin bzw. der Bürger von der Echtheit der Identität des Diensteanbieters (Unternehmens) überzeugen. Hierdurch kann auf andere personal- und kostenaufwendige Authentisierungsmaßnahmen sowie PIN/TAN-Verfahren verzichtet werden.

Der Wirtschaft entstehen daher ggf. Kosten für Berechtigungszertifikate und Lesegeräte, sofern sie den elektronischen Identitätsnachweis nutzen. Da sich die Preise für die Berechtigungszertifikate und Lesegeräte nach Angebot und Nachfrage richten, können hierfür

derzeit noch keine detaillierten Angaben gemacht werden. Einfache Basisleser werden voraussichtlich ab einem Preis von ca. 15 Euro auf dem Markt verfügbar sein. Sofern die Wirtschaft 500.000 Lesegeräte abnehmen würde, wäre hiermit eine Belastung von 7,5 Millionen Euro verbunden. Hinzukommen die Kosten für die Berechtigungszertifikate, die jedoch nicht beziffert werden können. Diesen Kosten stehen aber vorgenannte Einspar-potentiale für geringeren organisatorischen Aufwand und ein Gewinn an Sicherheit im Geschäftsverkehr gegenüber, sodass Auswirkungen auf Einzelpreise, das allgemeine Preis-niveau, insbesondere auf das Verbraucherpreisniveau, nicht zu erwarten sind. Eine genaue Quantifizierung der Kosten kann nicht erfolgen, da weder die Zahl der am elektronischen Identitätsnachweis teilnehmenden Wirtschaftszweige noch die Anzahl der Unternehmen ermittelt werden kann.

Eine weitere Senkung der Bürokratiekosten und –belastungen ergibt sich auch aus der Optimierung heutiger Antragsprozesse. Zukünftig werden ausschließlich auf elektronischem Wege Daten von der Ausweisbehörde zum Produzenten übertragen. An dieser Stelle wird auf die Erfahrungen und die Infrastruktur beim ePass zurückgegriffen. Dies trägt ebenfalls zur Verfahrensvereinfachung bei.

Diverse Prozesse, die als Informationspflichten für die Wirtschaft aufgeführt wurden, erfolgen in einem voll automatisierten Verfahren. Hierdurch entstehen lediglich laufende Kosten für die Wartung der Systeme. Ansonsten entstehen zur Implementierung für die Softwareentwicklung oder Einbindung in bestehende Prozesse Kosten. Die Kosten aller voll automatisierten Prozesse werden gesamt maximal im niedrigen einstelligen Millionenbereich erwartet.

Einhergehend mit den nach dem Personalausweisgesetz erwarteten Einsparungen an Bürokratiekosten für die Wirtschaft in Höhe von 129,23 Mio. € sind die Bürokratiekosten, die durch die Verordnung entstehen werden, vernachlässigbar.

Bürgerinnen und Bürger

Bei den neuen Informationspflichten handelt es sich vorwiegend um einfachere Abläufe, die keinen hohen Zeitaufwand beinhalten, bzw. um Abläufe die mit den bereits vorhandenen Informationspflichten (Ausweisbeantragung und –abholung) verknüpft sind. Insofern entstehen keine neuen Wege- und Wartezeiten. Lediglich die einzelnen Prozesse werden um wenige Minuten verlängert. Die einmalige Neusetzung einer PIN, wie auch das Verfahren bei fehlerhafter Eingabe und die Sperrung des Ausweises kann von zu Hause aus erledigt werden und ist nur notwendig, wenn der elektronische Identitätsnachweis genutzt werden soll.

Diesem geringen Zeitaufwand steht der Vorteil gegenüber, dass es der elektronische Identitätsnachweis den Ausweisinhabern ermöglicht, sich im Internet elektronisch auszuweisen – sowohl gegenüber Behörden im E-Government als auch gegenüber privat-wirtschaftlichen Dienstleistungsanbietern, beispielsweise bei Online-Shopping, Online-Banking oder Online-Auktionen. Diese vorgenannten Prozesse sind sowohl für die Anbieter als auch für die Bürgerinnen und Bürgern umständlich und zeitraubend. Der elektronische Identitätsnachweis vereinfacht insofern die Kommunikation und erhöht die Sicherheit der Geschäftsbeziehung als auch des Kontakts der Behörden im E-Government.

So entfallen für die Bürgerinnen und Bürger sowohl zeitaufwendige Authentisierungsverfahren (z.B. Post-Ident), als auch die Eingabe einer PIN/TAN bei jeder Online-Transaktion, da die Verifikation einmalig während einer Anmeldung über den elektronischen Identitätsnachweis erfolgt. Auch ist zu erwarten, dass Wegezeiten zu Behörden entfallen, da die Verwaltung im Wege des E-Government zahlreiche Prozesse anbieten wird, die mittels des elektronischen Identitätsnachweises über das Internet erledigt werden können. Dies führt somit zur Vereinfachung der Dienstleistung bzw. der Erfüllung einer Informationspflicht.

Verwaltung

Auch wenn für die Verwaltung zahlreiche neue Informationspflichten geschaffen werden, so kann die Verwaltung, insbesondere die Personalausweisbehörde, auf bestehenden Verfahren aus dem Passrecht aufbauen. Lediglich die neue Infrastruktur des elektronischen

Identitätsnachweises schafft neue Abläufe in der Verwaltung, die aber zum Teil im automatisierten Verfahren durchgeführt werden können.

Für die Verwaltung bedeuten die neuen Informationspflichten auf der einen Seite, dass neue Prozesse bei der Beantragung, Ausstellung und auch bei der Sperrung von Personalausweisen etabliert werden. Auf der anderen Seite erleichtert der Personalausweis zahlreiche Verwaltungsvorgänge, da viele durch Bund, Länder und Kommunen zu erbringende Dienstleistungen durch die elektronische Identifizierung online angeboten und abgewickelt werden können.

Die vom Auswärtigen Amt nach den Bestimmungen des Personalausweisgesetzes im Ausland bestimmten Auslandsvertretungen übernehmen ab dem 1.1.2013 ein vollkommen neues Aufgabenfeld. Hierzu muss das Auswärtige Amt eine neue zusätzliche Infrastruktur (IT-Verfahren, Liegenschaften, Personal usw.) aufbauen.

Tabelle I zu den Bürokratiebelastungen der Personalausweisverordnung
Normadressat: Wirtschaft

Lfd Nr.	Vorschrift	Art der Änderung	Informationspflicht	Fallzahl pro Jahr	Zeit in min	Lohnsatz in €/h	Zusatzkosten in €	Veränderung in €
1	§ 3 Abs. 3 i.V.m. Abs. 1 und 2	Bund-neu	Beantragung einer Zertifizierung	ca. 20	150	30,20	-	**1510**
2	§ 4 Abs. 2	Bund-neu	Dokumentationspflichten des Sperrnotrufs	32.500	3	30,20		**49.075**
3	§ 8 Abs. 4	Bund-neu	Hinterlegung von technischen Verbindungsparametern im DVDV	1	60	30,20		**30 (Einmalig)**
4	§ 9 Abs. 1 und 2	Bund-neu	Erstellung einer Qualitätsstatistik	1	360	31,80		**191**
5	§ 10	Bund-neu	Prüfung und Eingangsbestätigung des Antrags	6.500.000	0,02	31,80	bereits vorhanden	**68.900**
6	§ 14 Abs. 3 und § 5 Abs. 4 Satz 3	Bund-neu	Speicherung personenbezogener Daten und Führung einer Liste mit Sperrsummen	6.500.000	0,02	31,80	maximal 800.000	**68.900**
7	§ 15 Abs. 1 und § 16 Satz 1	Bund-neu	elektronische Übermittlung des Sperrkennwortes an Ausweisbehörde sowie Sperrsumme und Sperrschlüssel an den Sperrlistenbetreiber	6.500.000	0,02	31,80	maximal 800.000	**./. 68.900**
8	§ 15 Abs. 2 und § 16 Satz 3	Bund-neu	Anfrage durch Ausweishersteller bei Ausweisbehörde bzw. Sperrlistenbetreiber falls keine Rückmeldung erfolgt	500	3	31,80	-	**795**

9	§ 31	Bund-neu	Anzeige über die Bereitstellung von Berechtigungszertifikaten	600	90	41,29		**37.161**
10	§ 33 Satz 3 und 4	Bund-neu	Information bezügl. Zweifel über den Inhaber, die Gültigkeit oder den Umfang einer Berechtigung ggü. der Vergabestelle für Berechtigungszertifikate	12	10	30,20		**60**
11	§ 35 Abs. 1 und 2	Bund-neu	Abruf der allgemeinen Sperrliste	657.000	0,02	31,80	maximal 800.000	**6.964**

Tabelle II zu den Bürokratiebelastungen der Personalausweisverordnung
Normadressat: Bürgerinnen und Bürger

lfd. Nr.	Vorschrift	Art der Änderung	Informationspflicht*
1	§ 4 Abs. 1 Satz 1 Nr. 1 i.V.m § 17 Abs. 6 und § 18 Abs. 1	geändert	Identitätsnachweis, Bestätigung der Antragsangaben und Unterschrift durch antragstellende Person ***Fz = 6.500.000 mit einer Zeit von 4 Minuten***
2	§ 25 Abs. 1 Satz 2	Bund-neu	Identifizierung des Ausweisinhabers und Sperrung des elektronischen Identitätsnachweises nach Abhandenkommen des Personalausweises bei der Personalausweisbehörde (ggf. auch telefonisch) ***Fz = 32.500 mit einer Zeit von 5 Minuten***
3	§ 25 Abs. 1 i.V.m. Abs. 2	Bund-neu	Sperrung des elektronischen Identitätsnachweises nach Abhandenkommen des Personalausweises beim Sperrnotruf ***FZ. Max. 32.500 (0,5 % aller Ausweise (Diebstahl/Verlust); Dauer 3 Minuten***
4	§ 26 Abs. 1	Bund-neu	Antrag auf Entsperrung des gesperrten elektronischen Identitätsnachweises ***FZ 3.250 (=10% aller Verlust und Diebstähle) Dauer 10 Minuten (2/3 des Neuantrags) zzgl. 15 Minuten Wegezeit***

***Zeitermittlung erfolgt anhand standardisierter Vorgaben zur Bürokratiekostenmessung**

Tabelle III zu den Bürokratiebelastungen der Personalausweisverordnung Normadressat: Verwaltung

lfd. Nr.	Vorschrift	Art der Änderung	Informationspflicht
1	§ 3 Abs. 1 und 2	Bund-neu	Prüfung der Zertifizierungsvoraussetzungen und Erteilung eines Zertifikats das BSI
2	§ 4 Abs. 1	Bund-neu	Dokumentation der Personalausweisbehörde zu - Erklärungen des Ausweisinhabers im Rahmen der Antragstellung - die Übergabe des Briefs mit Geheimnummer und Sperrkennwort durch Ausweisbehörde an antragstellende Person , - die der Ein- und Ausschaltung der eID-Funktion nach Ausgabe und - Ausgabe des Personalausweises
3	§ 4 Abs. 3	Bund-neu	Dokumentation des Sperrlistenbetreibers zu - Sperrung des Personalausweises und - zur Entsperrung des Personalausweises
4	§ 5 Abs. 3 Nr. 2	Bund-neu	Aktualisierung der Sperrliste
5	§ 8 Abs. 1	keine	Übermittlung des Antragsdatensatzes an Ausweishersteller
6	§ 8 Abs. 4	Bund-neu	Hinterlegung von technischen Verbindungsparametern im DVDV
7	§ 15 Abs. 2	geändert	Unverzügliche Eingangsbestätigung bezüglich Sperrkennwort ggü. Ausweishersteller
8	§ 16 Satz 2	Bund-neu	Unverzügliche Eingangsbestätigung von Sperrsumme und Sperrschlüssel durch Sperrlistenbetreiber ggü. Ausweishersteller
9	§ 18 Abs. 3	Bund-neu	Anzeige der personenbezogenen Daten im Speicher- und Verarbeitungsmedium auf Antrag
10	§ 20 Abs. 1	Bund-neu	Identitätsprüfungsprüfung zur Einleitung der Neusetzung der Geheimnummer
11	§ 24 Abs. 1 und 2	Bund-neu	Führung einer Referenzliste und einer allgemeinen Sperrliste durch Sperrlistenbetreiber
12	§ 25 Abs. 2 und 3, § 26 Abs. 2 und 3	Bund-neu	Sperrungsmitteilung ggü. der Ausstellungsbehörde, Übermittlungs- und Dokumentationspflichten im Sperrverfahren
13	§ 27	Bund-neu	Bereitstellung eines Verfahrens zur Auskunft über Vorhandensein elektronischer Identitätsnachweise in der Sperrliste

B. Besonderer Teil

Zu § 1 (Begriffsbestimmungen)

Zu Absatz 1

Der Begriff der Sperrsumme ist im Rahmen der Regelungen zum Sperrmanagement zu definieren. Sie wird vom Ausweishersteller, dem Sperrnotruf oder Ausweisbehörden errechnet und vom Sperrlistenbetreiber zur Zuordnung genutzt.

Zu Absatz 2

Der Begriff des Sperrschlüssels ist im Rahmen der Regelungen zum Sperrmanagement zu definieren. Der Sperrschlüssel wird vom Ausweishersteller erzeugt und nur vom Sperrlistenbetreiber weiterverarbeitet.

Zu Absatz 3

In der Verordnung wird festgelegt, wer unter welchen Voraussetzungen Berechtigungszertifikate für den elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes ausstellen darf. In diesem Zusammenhang ist der Begriff des Berechtigungszeritifikateanbieters zu definieren.

Zu Absatz 4

Der Begriff des allgemeinen Sperrmerkmals war im Rahmen der Regelungen zum Sperrmanagement zu definieren. Das Sperrmerkmal wird vom Sperrlistenbetreiber errechnet und nur von Berechtigungszertifikateanbieter weiterverarbeitet.

Zu Absatz 5

Der Begriff des Sperrnotrufs ist im Rahmen der Regelungen zum Sperrmanagement zu definieren. Um eine zentrale, einfache und zeitlich hochverfügbare Sperrmöglichkeit zu schaffen, ist der Sperrnotruf neben den Personalausweisbehörden vorzusehen.

Zu Absatz 6

Der Begriff „XhD“ bezeichnet einen technischen Sachverhalt von hoher Bedeutung im Lebenszyklus des Personalausweises und wurde zum einheitlichen Verständnis legal definiert. Die Details sind in den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik festgelegt.

Zu Absatz 7

Der Begriff „OSCI-Transport“ bezeichnet einen technischen Sachverhalt von hoher Bedeutung im Lebenszyklus des Personalausweises und wurde zum einheitlichen Verständnis legal definiert.

Zu § 2 (Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik)

Das dem Personalausweis zugrunde liegende technische Konzept ist komplex und ist in den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zur Umsetzung durch die einzelnen Beteiligten detailliert niedergelegt. Datenschutz und Datensicherheit des technischen Systems „Personalausweis“ hängen wesentlich von ihrer Umsetzung nach dem Stand der Technik ab. Die Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik enthalten daher ausführliche Hinweise auf eine Umsetzung nach

dem Stand der Technik. § 2 enthält die zentrale Verweisungsnorm auf diese Richtlinien. Um das System flexibel zu halten und im Rahmen des technischen Fortschritts Weiterentwicklungen zu ermöglichen wird dynamisch auf die jeweils aktuelle im elektronischen Bundesanzeiger veröffentlichte Fassung der Richtlinien verwiesen.

Zu § 3 (Zertifizierung)

Zu Absatz 1

Die vorherige Überprüfung der Umsetzung der Anforderungen ist ein wichtiger Bestandteil des technischen Systems „Personalausweis“. Diese richtet sich nach den Zertifizierungsverfahren des Bundesamtes für Sicherheit in der Informationstechnik.

Die Richtigkeit und Sicherheit der Personalausweise hängt wesentlich von der Integrität der eingesetzten technischen Infrastrukturkomponenten ab. Soweit diese z. B. dezentral und in großen Stückzahlen bereitgestellt werden, ist daher die vorgabenkonforme Arbeitsweise zu bestätigen. Die Vorschrift legt die Einzelheiten der Prüfung und Bestätigung fest.

Zu Absatz 2

Die zu zertifizierenden Einzelkomponenten sind im Anhang 5 aufgeführt.

Zu Absatz 3

Absatz 3 regelt die Kostentragung.

Zu § 4 (Dokumentationspflichten)

Zu Absatz 1

Absatz 1 regelt ausführlich die Dokumentation einzelner Verfahrensschritte der Personalausweisbehörden.

Die ausführliche Dokumentation einzelner Verfahrensschritte einer Sperrung bei unterschiedlichen Beteiligten ermöglicht die Nachvollziehbarkeit und die Überprüfung der ordnungsgemäßen Durchführung einer Sperrung bei den Beteiligten. Die Vorschrift erweitert die Dokumentationspflichten der Personalausweisbehörde im Hinblick auf haftungsrelevante Handlungen im Zusammenhang mit dem elektronischen Identitätsnachweis. Dazu gehören die Beantragung, die Übergabe des Ausweises und der Geheimnummer sowie die Einschaltung, die Ausschaltung, die Sperrung und die Entsperrung des elektronischen Identitätsnachweises. Durch die Dokumentationspflicht besteht die Möglichkeit, Verantwortlichkeiten zum Zeitpunkt eines möglichen Schadenseintritts den Beteiligten zuzuweisen. Sie stellt damit die tatsächliche Grundlage für eine Beurteilung von Schadensfällen nach haftungsrechtlichen Regelungen dar.

Die Eintragung der Ausschaltung im Personalausweisregister hat Beweisfunktion und entlastet den Ausweisinhaber, da mit einem abgeschalteten elektronischen Identitätsnachweis keine missbräuchliche Identifizierung stattfinden kann.

Da die Dokumentation der Aus- oder Einschaltung und der Sperrung im Personal-ausweisregister der den Ausweis ausstellenden Personalausweisbehörde stattfindet und dort auch z. B. bei einem Umzug des Ausweisinhabers verbleibt, müssen andere Personalausweisbehörden – unabhängig davon, ob sie im Einzelfall zuständig sind

oder nicht – die ausstellende Behörde über die Aus- oder Einschaltung oder eine von ihnen initiierte Sperrung informieren.

Zu Absatz 2

Absatz 2 enthält die Dokumentationspflichten des Sperrnotrufs.

Zu Absatz 3

Absatz 3 regelt ausführlich die Dokumentationspflichten des Sperrlistenbetreibers. Bei der in Rede stehenden Sperrliste, handelt es sich um die allgemeine Sperrliste.

Zu § 5 (Speicherung und Löschung)

Die Vorschrift präzisiert auf Basis der Ermächtigung des § 34 Nr. 6 Buchstabe c) des Personalausweisgesetzes die Speicherungs- und Löschungsvorschrift für den Antrags- und Produktionsprozess. Dieser umfasst neben der Herstellung des Ausweiskörpers und der Personalisierung auch die Übermittlung von zugehörigen Informationen wie der Geheimnummer, dem Sperrkennwort, der Sperrsumme und des Sperrschlüssels sowie die Funktionsüberprüfung und Rückmeldung durch die Personalausweisbehörde und den Sperrlistenbetreiber. Danach sollen die Daten gelöscht werden, sobald sichergestellt ist, dass Daten und Dokument beim Sperrlistenbetreiber und bei der Personalausweisbehörde angekommen sind und der Produktionsauftrag ausgeführt wurde. Diese Lösung ist bürgerfreundlich, indem sie sicherstellt, dass keine erneute Erfassung der Antragsdaten aufgrund von Produktions- oder Übermittlungsfehlern erfolgen muss. Ausnahmen bestehen gemäß Personalausweisgesetz hinsichtlich der Speicherung einer Liste von Sperrnummern.

Für die Speicherung personenbezogener Daten bei einzelnen Verfahrensbeteiligten im Antrags- und Produktionsverfahren sowie im Sperrmanagement sind Speicherungs- und Löschungsfristen festzulegen. Ihre Dauer richtet sich nach der Erforderlichkeit der Nachweisführung zu den jeweiligen Daten.

Die Liste von Sperrsummen darf jedoch nicht mit Seriennummernlisten verbunden werden.

Zu § 6 (Erfassung der Anschrift)

Die Anschrift im Personalausweis dient seit jeher der physischen Auffindbarkeit der Person durch Behörden und ist daher eindeutig auszugestalten. Die Eindeutigkeit der Anschrift ist insbesondere für die Nutzung des elektronischen Identitätsnachweises erforderlich. Sie wird durch den Gemeindeschlüssel erreicht.

Zu § 7 (Qualitätssicherung des Lichtbildes und der Fingerabdrücke)

Zu Absatz 1

Die Vorschrift regelt verschiedene Möglichkeiten zur Beibringung oder Erstellung des Lichtbildes für den Ausweis. Neben der Möglichkeit, das Bild in Papierform einzureichen ist dabei auch die Möglichkeit der elektronischen Übermittlung etwa bei der Nutzung von Fotokabinen oder die Erstellung im Rahmen des Antragsprozesses (z. B. in Auslandsvertretungen, sog. Live Enrolement) vorzusehen.

Zu Absatz 2

Die Verwendung des Lichtbildes und der Fingerabdrücke als technisch abgleichbare biometrische Merkmale stellt strenge Qualitätsanforderungen an die Aufnahme dieser Merkmale, die vor einer Übernahme in den Ausweis technisch geprüft werden müssen.

Zu Absatz 3

Außerdem ist eine manuelle Prüfung des Lichtbildes mittels einer Fotomustertafel nach Anhang 3 Abschnitt 2 möglich. Auf Grund des Gleichlaufs der Anforderungen sind auch die Verfahren der biometrischen Erhebung und Nutzung entsprechend denen beim Pass geregelt.

Zu § 8 (Übermittlung)

Zu Absatz 1

Mit der Einführung des elektronischen Reisepasses wurde das Antragsverfahren auf eine elektronische Erfassung und Übermittlung umgestellt. Diese Umstellung setzt sich mit der Einführung elektronisch auswertbarer biometrischer Merkmale im Personalausweis fort, wobei insbesondere aus Kostengründen weitgehender Gleichlauf mit dem Reisepass herzustellen ist. Die Regelungen entsprechen daher den Regelungen der Passdatenerfassungs- und Übermittlungsverordnung.

Zu Absatz 2 bis Absatz 4

Die Sicherstellung von Datenschutz und Datensicherheit, hier insb. von Authentizität und Integrität der Datenerfassung und –übermittlung, ist wesentliches Ziel des einzuführenden elektronischen Verfahrens. Die Erreichung dieser Ziele wird im technischen System „Personalausweis“ durch die Verwendung von Public Key Infrastrukturen (PKI) sichergestellt. Die Vorschriften regeln Einzelheiten zur Ausgestaltung dieser PKI.

Zu § 9 (Qualitätsstatistik)

Der Umgang mit biometrischen Merkmalen in der Ausweisproduktion und -kontrolle ist vergleichsweise neu. Zur optimalen Anpassung der Produktion der Personalausweise soll die Qualität der Lichtbilder und Fingerabdruckdaten auf der Basis von § 34 Nummer 2 des Personalausweisgesetzes statistisch ausgewertet werden. Die Regelung entspricht der im Passrecht.

Zu § 10 (Eingang der Antragsdaten)

Die Vorschrift stellt eine Kontrolle des elektronischen Übertragungsweges hinsichtlich Integrität und Authentizität der übermittelten Daten sicher.

Zu § 11 (Muster für den Personalausweis)

Die physische Ausgestaltung der Ausweiskarte ist in Anhang 1 konkretisiert. Dabei ergeben sich insbesondere durch das neue Format in Kreditkartengröße und ein neues Herstellungsmaterial erhebliche Unterschiede zur bisherigen Ausweiskarte. Das kleinere Format mit den Abmessungen 85,60 x 53,98 x 0,76 mm ist international nach ISO 7810 als Format "TD-1" standardisiert und mittlerweile auch für Identitäts- und Reisedokumente verbreitet (z.B. für Identitätskarten in Belgien, Polen, Österreich

und der Schweiz sowie für die "Passport Card" der USA). Zahlreiche Bürger hatten sich in Petitionen für eine Änderung des Formats ausgesprochen. Das Material ergab sich u.a. aus den Anforderungen an die Fälschungssicherheit, die Haltbarkeit und die Integration eines elektronischen Speicher- und Verarbeitungsmediums für die technisch auswertbaren biometrischen Merkmale, den elektronischen Identitätsnachweis und die qualifizierte elektronische Signatur. Bei der graphischen Gestaltung der neuen Ausweiskarte musste dem verkleinerten Format Rechnung getragen werden, die maschinenlesbare Zone befindet sich nun auf der Rückseite.

Bei der Gestaltung der Ausweiskarte wurde sich an anerkannten Merkmalen des bisherigen Personalausweises orientiert. Deshalb zeigt die Vorderseite der Ausweiskarte im Hintergrund wie bisher neben Guillochenmustern den Bundesadler aus dem großen Bundessiegel (vergl. die Bildtafel zu den Richtlinien für die Anfertigung von Dienstsiegeln und Verwendung des Bundesadlers auf amtlichen Schildern und Drucksachen vom 4. März 1950 (Gemeinsames Ministerialblatt Nr. 2 vom 18. April 1950 Seite 18)). Die gewählte Form zeigt frei schwebend den einköpfigen Adler, dessen Kopf nach rechts gewendet, die Flügel offen, doch sind die Spitzen des Gefieders (sieben an der Zahl) nach außen gerichtet. Diese Adlerdarstellung steht in Kontinuität zur Ausführung des bisherigen Personalausweises und unterstreicht wegen des Bezuges zum Bundessiegel dessen urkundlichen Charakter.

Die Rückseite wurde graphisch neu gestaltet. Den Hintergrund für die variablen Bestandteile bildet nun eine Darstellung des Brandenburger Tores in Berlin, wiederum flankiert von einem Guillochenmuster. Das Brandenburger Tor war Sinnbild der Teilung Deutschlands und des Willens zu Ihrer Überwindung. Es steht heute für die Vollendung der Einheit und Freiheit Deutschlands in freier Selbstbestimmung und entwickelt Symbolcharakter als Zeichen der nationalen Identität, weshalb es u.a. auch auf den deutschen Euromünzen abgebildet ist.

An der Adressänderung mittels Aufkleber musste mangels anderer praxistauglicher Lösungen festgehalten werden. Die Aufbringung der Adresse ist eine fast nur in Deutschland praktizierte Lösung, die auch den konsequent dezentralen Strukturen der Pass- und Personalausweisbehörden geschuldet ist. In anderen Staaten werden diese Daten über zentral abrufbare Register für Behörden zum Abruf bereitgehalten.

Die im elektronischen Speicher- und Verarbeitungsmedium gespeicherten Daten zur elektronischen Identitätsfunktion sind identisch mit den auf dem Ausweis aufgedruckten Daten. Sofern also aufgrund von Platzmangel Daten auf dem Ausweis gekürzt dargestellt werden, sind diese auch nur in der gekürzten Form abgespeichert.

Zu § 12 (Muster für den vorläufigen Personalausweis)

Der vorläufige Personalausweis hat sich anders als der Personalausweis kaum verändert. Es wurde lediglich ein Feld für die wieder eingeführten Ordens- und Künstlernamen sowie für die ausstellende Behörde vorgesehen.

Das Muster hat die Größe 125 mm x 88 mm.

Zu § 13 (Schnittstelle des elektronischen Speicher- und Verarbeitungsmediums)

Die Vorschrift legt die grundlegende Ausgestaltung der elektronischen Funktionalität bzw. der Schnittstelle des elektronischen Speicher- und Verarbeitungsmediums des Personalausweises fest. Die Vorschrift ergänzt die Musterdarstellung, da der Chip aufgrund der kontaktlosen Schnittstelle nicht optisch zu erkennen ist. Diese Art der technischen Ausgestaltung ist maßgeblich für die einzusetzenden Übertragungsprotokolle und Sicherheitsverfahren.

Zu § 14 (Speicherung von personenbezogenen Daten; Zugriffsschutz)

Zu Absatz 1

Absatz 1 enthält eine wichtige technische Vorgabe zu Datenschutz und Datensicherheit, indem er für alle personenbezogenen Daten im Personalausweis den höchsten (zertifikatsbasierten) Zugriffsschutzstandard vorsieht. Dies ist auf Grund der Verwendung des Personalausweises über öffentliche Kommunikationsverbindungen geboten. Damit unterscheidet sich der Personalausweis vom Reisepass, der auf Grund von ICAO-Vorgaben diesen Standard nur für die Fingerabdrücke vorsieht. Nr. 3 enthält eine zentrale Vorschrift zur Ausgestaltung von IT-Sicherheit und Datenschutz im Personalausweis, indem bei allen Übertragungsvorgängen von personenbezogenen Daten zwischen Karte, Lesegeräten und eID-Servern konsequent Verschlüsselung eingesetzt werden muss.

Zu Absatz 2

Absatz 2 stellt sicher, dass das Dokument so produziert wird, dass die Grundregeln der Verwaltung von Zugriffrechten auf personenbezogene Daten in Personalausweisen durch Behörden und private Stellen implementiert werden. Die Regelung sieht vor, dass die notwendigen technischen Grundlagen für die Umsetzung der gesetzlichen Regelungen zur Zugriffsverwaltung bei der Produktion bereitgestellt werden.

Zu § 15 (Übermittlung und Übersendung des Sperrkennworts an die Personalausweisbehörde)

Zu Absatz 1

Absatz 1 regelt die Auslieferung des zum Ausweis gehörigen Sperrkennworts an die Ausweisbehörden. Die Ermächtigung ergibt sich aus § 34 Nr. 6 Buchstabe c) des Personalausweisgesetzes.

Zu Absatz 2

Die Regelung dient einer zügigen, aber gleichwohl vollständigen Abwicklung des Auslieferungsverfahrens der Sperrkennwörter. Da an die Bestätigung auch die Löschung der Daten beim Ausweishersteller geknüpft ist, war eine kurzfristige Nachfrage auch unter dem Gesichtspunkt der Datensparsamkeit einzuführen.

Zu § 16 (Übermittlung der Sperrsumme und des Sperrschlüssels an den Sperrlistenbetreiber)

Die Vorschrift regelt die Auslieferung der für eine Sperrung erforderlichen Daten Sperrschlüssel und Sperrsumme an den Sperrlistenbetreiber. Die Pflicht zur Bestätigung war im Hinblick auf eine zügige aber vollständige Abwicklung des Produktionsverfahrens geboten.

Zu § 17 (Übersendung der Geheimnummer, der Entsperrnummer und des Sperrkennworts)

Zu Absatz 1 und Absatz 3

Neu im Antragsverfahren für Personalausweise ist die Benachrichtigung der antragstellenden Person durch den Ausweishersteller, dass der Ausweis an die Personalausweisbehörde ausgeliefert wurde. Dies ist bürgerfreundlich und ermöglicht die sichere Übersendung der Geheimnummer, Entsperrnummer und des Sperrkennwortes auf vom Dokument getrenntem Wege. Der Brief ist durch geeignete Maßnahmen gegen eine Kenntnisnahme der Nummern durch Dritte, die etwa den Umschlag durchleuchten oder öffnen, zu schützen. Da der Brief im Rücklauffall an die Personalausweisbehörde zugestellt wird, ist sicherzustellen, dass trotz Öffnung des Briefes die Nummern auch den Mitarbeitern der Personalausweisbehörde nicht bekannt werden.

Zu Absatz 2

Im Inland wie im Ausland ist sicherzustellen, dass Ausweis und Brief nie gemeinsam mit einer Postsendung versandt werden, um einen Missbrauch bei einem Abhandenkommen der Sendung zu vermeiden.

Zu Absatz 4

In Ausnahmefällen etwa, wenn die antragstellende Person nicht sicherstellen kann, dass der Brief ihr unter der angegebenen Anschrift auch wirklich zugeht, kann der Ausweishersteller den Brief auch an die Personalausweisbehörde zur Übergabe senden. Dies geschieht aufgrund der angegebenen Rücksendeadresse auch dann, wenn sich der Brief bei der antragstellenden Person als postalisch unzustellbar erweist. Die Personalausweisbehörde soll diesen Brief öffnen, den Inhalt [das Anschreiben und die gegen Kenntnisnahme Dritter geschützten Informationen (Geheimnummer, Entsperrnummer und Sperrkennwort)] sicher verwahren und sodann der antragstellenden Person übergeben. In diesen Fällen entfällt die Information der Bürgerinnen und Bürger über die Auslieferung des Ausweises und der Ausweisinhaber trägt das zusätzliche Risiko Geheimnummer und Ausweisdokument gleichzeitig bei sich tragen zu müssen. Darauf ist er durch das bereitgestellte Informationsmaterial hinzuweisen.

Zu Absatz 5

Da der elektronische Identitätsnachweis erst ab 16 Jahre genutzt werden kann, entfällt die Zusendung des Briefes mit der Geheimnummer, Entsperrnummer und dem Sperrkennwort bei Antragsstellung vor dem Erreichen der Altersgrenze von 15 Jahren und neun Monaten mangels Erforderlichkeit. Bei einer früheren Versendung entsteht ein mit fortschreitender Zeitdauer steigendes Risiko, dass der Brief mit der Geheimnummer verloren geht.

Zu Absatz 6

Geht der Brief auf dem Postwege verloren, kann ein neuer Personalausweis beantragt werden. Da der Antragsdatensatz noch in der Personalausweisbehörde vorhanden ist, kann dieser erneut von dort aus übermittelt werden. Um einem erneuten Verlust vorzubeugen, wird der Brief in diesem Fall an die Personalausweisbehörde zur Übergabe versandt.

Zu Absatz 7

Zu Dokumentationszwecken, dass die Auslieferung des Dokuments (Besitz) und der zugehörigen Daten (Wissen) erfolgt ist und der elektronische Identitätsnachweis eingesetzt werden kann, ist der Zugang des Briefes bei Abholung des Dokuments zu bestätigen.

Zu § 18 (Aushändigung des Personalausweises)

Zu Absatz 1 und 2

Absatz 1 und 2 legen fest, dass der Personalausweis nur mit ausgeschalteter elektronischer Identitätsfunktion ausgegeben werden darf, sofern die antragstellende Person dies ausdrücklich wünscht oder aber den Erhalt des Briefs mit der Geheimnummer nicht bestätigt.

Zu Absatz 3

Im Rahmen des elektronischen Identitätsnachweises sind Daten auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeichert. Da der Ausweisinhaber diese ohne gültiges Berechtigungszertifikat nicht auslesen kann, schafft Absatz 3 Transparenz für den Ausweisinhaber, indem er einen Auskunftsanspruch auf die im elektronischen Speicher- und Verarbeitungsmedium gespeicherten auslesbaren Daten gegenüber der Personalausweisbehörde statuiert. § 5 Absatz 5 des Personalausweisgesetzes führt die im elektronischen Speicher- und Verarbeitungsmedium gespeicherten Daten auf, die ausgelesen werden können. Darüber hinaus enthält das Speichermedium auch Daten im Zusammenhang mit dem elektronischen Identitätsnachweis (z.B. Geheimnummer, privater Schlüssel) die aus Sicherheitsgründen nicht ausgelesen werden können. Der Auskunftsanspruch war daher entsprechend zu begrenzen.

Zu Absatz 4

Absatz 4 sorgt für die vorgeschriebene Verwendung zertifizierter Lesegeräte und stellt sicher, dass tatsächlich die Ausweisdaten und ausschließlich diese vom Gerät angezeigt werden.

Zu § 19 (Änderung der Anschrift)

Zu Absatz 1

Absatz 1 regelt die Ausstellung des Adressänderungsaufklebers durch die Personalausweisbehörden. Dabei ist neben der Anschrift die Seriennummer aufzunehmen, die eine eindeutige Zuordnung des Aufklebers zum Dokument sicherstellt. Bei der Personalisierung des Aufklebers ist vorrangig Tintenstrahldrucktechnik zu verwenden. Andere Drucktechniken sind jedoch zulässig. Nach der Personalisierung ist der Aufkleber zu siegeln. Die beschriebene Abfolge der Verfahrensschritte dient der Sicherung gegen Fälschungen oder nachträgliche

Veränderungen. Die optionale Anbringung einer Schutzfolie durch die Personalausweisbehörde soll sicherstellen, dass kein Austausch von Aufklebern stattfindet. Die Verwendung einer Schutzfolie soll zudem vor Abrieb und eingeschränkter Lesbarkeit schützen. Abmessungen des Aufklebers: 17 Millimeter x 45 Millimeter.

Zu Absatz 2

Absatz 2 regelt die Anschriftenänderung im elektronischen Speicher- und Verarbeitungsmedium. Die Änderung gilt für die hoheitliche Auslesung und den elektronischen Identitätsnachweis gleichermaßen. Für die Änderung sind spezielle hoheitliche Zertifikate erforderlich.

Zu Absatz 3

Absatz 3 legt mit der Verpflichtung zum Einsatz zertifizierter Geräte und hoheitlicher Zertifikate den technisch-organisatorischen Sicherheitsstandard des Änderungsvorgangs fest.

Zu § 20 (Neusetzung und Änderung der Geheimnummer)

Zu Absatz 1

Absatz 1 sieht vor, dass der Ausweisinhaber vor erstmaliger Nutzung seines elektronischen Identitätsnachweises die übersandte (Transport-)Geheimnummer ändern muss. Dieses Verfahren ist von qualifizierten elektronischen Signaturkarten bekannt und war hier zu übernehmen, da der elektronische Identitätsnachweis zur Identifizierung im Rahmen der Ausstellung qualifizierter Zertifikate dienen kann und daher mindestens die gleiche Sicherheit bieten muss.

Für den Fall, dass der Ausweisinhaber seine Geheimnummer nicht mehr kennt, ist eine Neusetzung ausschließlich in der Personalausweisbehörde möglich. Die Personalausweisbehörden benötigen dafür spezielle hoheitliche Berechtigungszertifikate. Die Personalausweisbehörden sollen den Ausweisinhaber bei der Neusetzung der Geheimnummer darauf hinweisen, dass aus Sicherheitsgründen keine Zahlenkombination verwandt werden sollte, die auf dem Ausweis aufgedruckt ist. Vor der Neusetzung ist eine Identifizierung des Ausweisinhabers zwingend erforderlich, um den Missbrauch abhanden gekommener Dokumente zu unterbinden.

Zu Absatz 2

Absatz 2 regelt die Möglichkeit der Änderung der Geheimnummer durch den Ausweisinhaber, wenn die Geheimnummer dem Ausweisinhaber noch bekannt ist.

Zu Absatz 3

Absatz 3 legt mit der der Verpflichtung zum Einsatz zertifizierter Geräte und hoheitlicher Zertifikate den technisch-organisatorischen Sicherheitsstandard des Neusetzungs- und Änderungsvorgangs fest.

Zu § 21 (Mehrfache Fehleingabe der Geheimnummer)

Zu Absatz 1

Die Möglichkeit der Geheimnummerneingabe war aus Sicherheitsgründen auf drei Versuche zu beschränken. Um eine unbemerkte Lahmlegung des elektronischen Identitätsnachweises durch die mehrfache Falscheingabe von Geheimnummern zu unterbinden, muss der Ausweisinhaber vor dem dritten Eingabeversuch seine nur auf

dem Dokument aufgedruckte Zugangsnummer eingeben, um den dritten Eingabeversuch freizuschalten.

Zu Absatz 2

Die Regelung sieht eine Entsperrung nach dreimaliger Falscheingabe der Geheimnummer durch Eingabe der Entsperrnummer vor. Dieses Verfahren ist von Mobilfunkkarten weithin bekannt und etabliert. Die Entsperrnummer kann aus Sicherheitsgründen maximal zehn Mal verwendet werden.

Zu § 22 (Nachträgliches Aus- und Einschalten)

Zu Absatz 1 und Absatz 2

Die Ein- und Ausschaltung des elektronischen Identitätsnachweises ist nach dem Personalausweisgesetz jederzeit möglich. Die Absätze 1 und 2 regeln das Verfahren, wenn die Aus- oder Einschaltung nach der initialen Ausgabe des Dokuments stattfindet.

Zu Absatz 3

Absatz 3 legt mit der der Verpflichtung zum Einsatz zertifizierter Geräte und hoheitlicher Zertifikate den technisch-organisatorischen Sicherheitsstandard des Ein- und Ausschaltvorgangs fest.

Zu § 23 (Voraussetzungen für die Nutzung bei dem Ausweisinhaber)

Zu Absatz 1

Absatz 1 sieht vor, dass der Ausweisinhaber vor erstmaliger Nutzung seines elektronischen Identitätsnachweises die übersandte (Transport-)Geheimnummer ändern muss. Dieses Verfahren ist von qualifizierten elektronischen Signaturkarten bekannt und war hier zu übernehmen, da der elektronische Identitätsnachweis zur Identifizierung im Rahmen der Ausstellung qualifizierter Zertifikate dienen kann und daher mindestens die gleiche Sicherheit bieten muss.

Zu Absatz 2

Die Vorschrift gibt Hinweise darauf, welche Systemvoraussetzungen für eine optimal sichere Verwendung des elektronischen Identitätsnachweises vom Ausweisinhaber bereitgestellt werden sollen.

Zu § 24 (Referenzliste; allgemeine Sperrliste)

Zu Absatz 1

Die Referenzliste ist eine zur Sperrung elektronischer Identitätsnachweise erforderliche Speicherung bestimmter ausweisbezogener Daten beim Sperrlistenbetreiber. Es findet keine Abfrage oder Nutzung durch Dritte oder Weitergabe der Daten aus der Referenzliste statt.

Zu Absatz 2

Der Begriff allgemeine Sperrliste bezeichnet eine zur Sperrung elektronischer Identitätsnachweise erforderliche Speicherung bestimmter ausweisbezogener Daten beim Sperrlistenbetreiber. Sie wird aus Daten der Referenzliste errechnet und wird

anders als die Sperrliste ausschließlich an die Berechtigungszertifikateanbieter zur Errechnung dienstespezifischer Sperrlisten weitergegeben.

Zu § 25 (Sperrung des elektronischen Identitätsnachweises)

Zu Absatz 1

Absatz 1 regelt die Pflicht des Ausweisinhabers zur eigenen Sicherheit und zur Vertrauenswürdigkeit des Gesamtsystems beizutragen, indem er den elektronischen Identitätsnachweis sperren lässt, wenn sein Personalausweis (Besitz) abhanden gekommen ist. Die Sperrung erfolgt somit spätestens bei Beantragung eines neuen Ausweises, da bei diesem Vorgang die Verlustmeldung entgegengenommen wird. Diese Verfahrensweise ist dem Grunde nach auch von anderen Kartensystemen bekannt und etabliert.

Unabhängig davon, ob eine Sperrung telefonisch oder persönlich erfolgt, ist eine hinreichende Identifizierung des Ausweisinhabers zum Schutz gegen Missbrauch der Sperrfunktion durchzuführen.

Zu Absatz 2 und Absatz 3

Die Absätze 2 und 3 regeln im Einzelnen die Voraussetzungen einer Sperrung und die Vorgehensweise seitens des Sperrnotrufs oder der Personalausweisbehörde. Für Personalausweisbehörden, die einen zu sperrenden elektronischen Identitätsnachweis nicht selbst ausgestellt haben, ist ein Informationsverfahren einzuführen, da nur die ausstellende Personalausweisbehörde in ihrem Register über das für die Sperrung erforderliche Sperrkennwort verfügt.

Zu § 26 (Entsperrung des elektronischen Identitätsnachweises)

Die Norm regelt das Verfahren der Entsperrung eines elektronischen Identitätsnachweises. Es orientiert sich im Wesentlichen an dem Verfahren für die Sperrung in § 25. Auf die dortige Begründung wird verwiesen. Unterschiede bestehen dahingehend, dass eine Entsperrung über den Sperrnotruf nicht erfolgen kann und ein persönliches Erscheinen des Ausweisinhabers in der Personalausweisbehörde erforderlich ist.

Zu § 27 (Auskunft über Sperrung)

Die Regelung normiert Auskunftsansprüche einerseits für die Ausweisinhaber hinsichtlich des aktuellen Sperrstatus ihres elektronischen Identitätsnachweises. Darüber hinaus besteht ein Auskunftsanspruch für ausstellende Personalausweisbehörden.

Zu § 28 (Antrag)

Zu Absatz 1

Die Vorschrift regelt die formalen Voraussetzungen für die Beantragung von Berechtigungen und die Art der Identifizierung der Diensteanbieter. Insbesondere die Identifizierung ist wesentlicher Vertrauensanker des Verfahrens und in vielfältiger Sicht vergleichbar mit der Identifizierung der Ausweisinhaber durch die Personalausweisbehörden bei der Antragstellung. Diese Vorschrift konkretisiert die

gesetzliche Regelung des § 21 des Personalausweisgesetzes. Die Antragsvoraussetzungen nach Absatz 1 knüpfen an die folgenden Regelungen des § 21 des Personalausweisgesetzes an:

- Ziffer 1 an § 21 Absatz 1 Satz 1 sowie Absatz 2 Satz 1 Nummer 5 des Personalausweisgesetzes,
- Ziffer 2 an § 21 Absatz 1 Satz 1 sowie Absatz 2 Satz 1 Nummer 5 des Personalausweisgesetzes,
- Ziffer 3 an § 21 Absatz 1 Satz 1 sowie Absatz 2 Satz 1 Nummer 5 des Personalausweisgesetzes,
- Ziffer 4 an § 21 Absatz 2 Satz 1 Nummer 5 des Personalausweisgesetzes,
- Ziffer 5 an § 21 Absatz 2 Satz 1 Nummer 1, 2 und 5 des Personalausweisgesetzes,
- Ziffer 6 an § 21 Absatz 2 Satz 1 Nummer 1 und 2 des Personalausweisgesetzes,
- Ziffer 7 an § 21 Absatz 2 Satz 1 Nummer 3 des Personalausweisgesetzes,
- Ziffer 8 an § 21 Absatz 2 Satz 1Nummer 5 des Personalausweisgesetzes
- Ziffer 9 an § 21 Absatz 2 Satz 1 Nummer 5 des Personalausweisgesetzes.

Zu Absatz 2

Die unterschiedlichen Identifizierungsmöglichkeiten des Absatzes 2 liegen in der Wahl des Antragstellers, soweit die technischen Möglichkeiten der jeweiligen Identifizierungsart durch die Vergabestelle für Berechtigungszertifikate geschaffen worden sind.

Zu § 29 (Anforderungen an Datenschutz und -sicherheit)

Zu Absatz 1

Die Regelung präzisiert die Erteilungsausschlüsse für Berechtigungen nach § 21 Absatz 2 Satz 1 Nummer 4 des Personalausweisgesetzes. Die genannten Fallgruppen stellen wesentliche Anforderungen an Datenschutz und Datensicherheit dar.

Nummer 1 konkretisiert die Ausschlussklausel des § 21 Absatz 2 Satz 1 Nummer 2 des Personalausweisgesetzes im Hinblick auf § 29 des Bundesdatenschutzgesetzes.

Nummer 2 grenzt die Datenübermittlung auf Diensteanbieter mit angemessenem Datenschutzniveau ein. Ein angemessener Datenschutzstandard kann sich sowohl aus Artikel 25 Absatz 1 als auch aus Artikel 25 Absatz 6 (Feststellung im Komitologieverfahren) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ergeben.

Die Nummern 3 und 4 stellen auf besondere Datenschutzrisiken durch Einschaltung eines Dritten (Auftragsdatenverarbeiters) ab. Durch Nummer 3 wird eine klare Zuweisung der Verantwortlichkeiten erreicht. Nummer 4 legt das vom Bundesamt für Sicherheit in der Informationstechnik definierte technisch-organisatorische Anforderungsniveau fest.

Zu Absatz 2

Absatz 2 regelt insbesondere die technischen Anforderungen an die Diensteanbieter und Dritte, die technische Dienstleistungen für Diensteanbieter erbringen (Auftragsdatenverarbeiter).

Zu Absatz 3

Die Vorschrift konkretisiert die Zusammenarbeit zwischen der Vergabestelle für Berechtigungszertifikate und den zuständigen Datenschutzaufsichtsbehörden.

Zu § 30 (Öffentliche Liste der Berechtigungen)

Die Norm sorgt für Transparenz bei erteilten Berechtigungszertifikaten und berechtigten Diensteanbietern, indem sie die Bereitstellung einer öffentlichen Liste der Berechtigungen festlegt. Die Ausweisinhaber werden dadurch in die Lage versetzt, bei Zweifeln an der Gültigkeit oder der zweckgebundenen Verwendung eines Berechtigungszertifikats, das Zertifikat und seine Erteilungszusammenhänge zu prüfen und gegebenenfalls auch von der zuständigen Datenschutzaufsichtsbehörden nachprüfen zu lassen.

Zu § 31 (Anzeige der Ausgabe von Berechtigungszertifikaten)

Die Bereitstellung von Berechtigungszertifikaten kann direkt durch die Vergabestelle für Berechtigungszertifikate oder - da es sich um marktübliche Zertifikate handelt - unter Berücksichtigung des Marktmodells nach Signaturrecht durch private Berechtigungszertifikateanbieter erfolgen. Im letzteren Fall hat die Vergabestelle für Berechtigungszertifikate dafür zu sorgen, dass entsprechende Berechtigungszertifikate am Markt verfügbar sind und über jederzeit öffentlich erreichbare Kommunikationsverbindungen zur Verfügung gestellt werden. Auf Grund der Vergleichbarkeit der Anforderungen wird inhaltlich auf das Anzeigeverfahren nach § 4 Absatz 3 des Signaturgesetzes zurückgegriffen. Da die Behörde nach § 3 des Signaturgesetzes über die fachlichen und organisatorischen Möglichkeiten der Prüfung verfügt, wird auch das Anzeigeverfahren selbst bei ihr durchgeführt. Die erfolgte Anzeige ist lediglich zusätzlich der Vergabestelle für Berechtigungszertifikate mitzuteilen.

Im Rahmen des § 31 Nummer 2 ist der Vergabestelle für Berechtigungszertifikate nicht die Dokumentation für die signaturrechtliche Anzeige bei der Bundesnetzagentur vorzulegen.

Zu § 32 (Beachtung der Anforderungen des Inhabers der Wurzelzertifikate)

Eine Signierung der eigenen Zertifikate durch den Inhaber der Wurzelzertifikate ist notwendige technische Voraussetzung für die Ausstellung von Berechtigungszertifikaten. Das Bundesamt für Sicherheit in der Informationstechnik als Inhaber der Wurzelzertifikate setzt Richtlinien für einen sicheren und effizienten Ablauf der Bereitstellung von Berechtigungszertifikaten.

Zu § 33 (Beachtung der Berechtigung durch den Berechtigungszertifikateanbieter)

Um eine Durchsetzung des inhaltlichen und zeitlichen Umfangs der Berechtigungen sicherzustellen, sind die Berechtigungszertifikateanbieter an die Vorgaben der Vergabestelle für Berechtigungszertifikate wie sie in den erteilten Berechtigungen vorliegen zu binden.

Zu § 34 (Gültigkeitsdauer von Berechtigungszertifikaten)

Die Gültigkeitsdauer von Berechtigungszertifikaten bestimmt maßgeblich, wie schnell rechtswidrig handelnde Diensteanbieter, denen die Berechtigung entzogen worden ist, von einer weiteren Datenerhebung ausgeschlossen und damit die Ausweisinhaber geschützt werden können. Da das Einsatzumfeld des elektronischen Identitätsnachweises Infrastrukturcharakter hat und daher sehr variabel und weit ist, war eine allgemeine Festlegung nicht sachgerecht. Die Gültigkeitsdauer wird daher nunmehr im Einzelfall von der Vergabestelle für Berechtigungszertifikate getroffen, wobei sie sich in den Grenzen der Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik bewegen kann. Das Bundesamt für Sicherheit in der Informationstechnik hat die maximalen Gültigkeitsdauern für bestimmte Einsatzszenarien unter Abwägung des Risikos in seinen Richtlinien nach § 34 Satz 2 festzulegen.

Zu § 35 (Speicherung, Abruf und Verwendung von Daten durch Berechtigungszertifikateanbieter)

Die Norm regelt einerseits die Abrufpflicht für aktuelle Sperrlisten, um eine angemessene Zeitdauer der Sperrung von elektronischen Identitätsnachweisen sicherzustellen. Andererseits beschränkt sie die Verwendung und Speicherung der zur Sperrung erforderlichen Daten bei den Berechtigungszertifikateanbietern.

Die Erzeugung dienstespezifischer Sperrlisten ist – neben der Bereitstellung von Berechtigungszertifikaten – fakultativer Vertragsbestandteil zwischen Berechtigungszertifikateanbieter und Diensteanbieter. Der Bezug der Sperrlisten liegt im Eigeninteresse der Diensteanbieter, um der Akzeptanz abhanden gekommener Ausweise beim elektronischen Identitätsnachweis praktisch durch Prüfung der Sperrliste entgegenwirken zu können.

Zu § 36 (Ausgabe von hoheitlichen Berechtigungszertifikaten)

Die Vorschrift regelt die Ausgabe hoheitlicher Berechtigungszertifikate an den definierten Kreis der Berechtigten. Eine Erweiterung dieses Kreises findet durch die Norm nicht statt. Da unterschiedliche Berechtigte die Zertifikate aus verschiedenen Quellen beziehen sollen, war die Bestimmung der ausgebenden Stelle flexibel zu halten. Sie wird durch eine Veröffentlichung im elektronischen Bundesanzeiger transparent gemacht.

Zu § 37 (Übergangsregelungen)

Zu Absatz 1

Die Vordrucke für vorläufige Personalausweise haben sich nur unwesentlich verändert. Der wirtschaftlich sinnvollen Weiterverwendung alter, bereits ausgelieferter Formulare zur Erstellung vorläufiger Personalausweise steht daher für die Dauer eines Jahres nichts im Wege. Dies gilt insbesondere für die Fälle, in denen die antragstellende Person keinen Ordens- und Künstlernamen bei der Antragstellung angibt. Bei Bedarf kann auf dem alten Vordruck auch unter Eintragung der Überschrift „Ordens- und Künstlername“ mittels Tintenstrahldrucktechnik ein Ordens- und Künstlername auf der Rückseite eingetragen werden.

Zu Absatz 2

Mit dieser Verordnung ist ein Wechsel der zu verwendenden Signaturkarten für die Authentisierung der Personalausweisbehörden beim Ausweishersteller im Antragsverfahren vorgesehen. Alte Karten können aus wirtschaftlichen Gründen für die Dauer ihrer Gültigkeit weiter verwendet werden. Die im Feld befindlichen (proprietären) Signaturverfahren der Bundesdruckerei werden für eine gewisse Übergangszeit fortgeführt, damit ein fließender Übergang zum Einsatz des DVDV ermöglicht wird.

Zu § 38 (Inkrafttreten)

Das Inkrafttreten der Verordnung ist zeitgleich mit dem Inkrafttreten ihrer Ermächtigungsgrundlage in § 34 des Personalausweisgesetzes vorgesehen.

Anlage

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKR-Gesetz

NKR-Nr. 1146: Verordnung über Personalausweise und den elektronischen Identitätsnachweis

Der Nationale Normenkontrollrat hat das oben genannte Regelungsvorhaben auf Bürokratiekosten geprüft, die durch Informationspflichten begründet werden.

Mit dem Regelungsvorhaben werden für die Wirtschaft 11 Informationspflichten eingeführt. Hierdurch entstehen jährliche Bürokratiekosten in Höhe von rund 300 Tsd. Euro. Der Schwerpunkt der jährlichen Kostenbelastung liegt bei den Informationspflichten des Ausweisherstellers. Daneben entstehen einmalig Bürokratiekosten in Höhe von rund 10 Mio. Euro für die Beschaffung von Software durch den Ausweishersteller sowie für die Beschaffung von Kartenlesegeräten durch die Unternehmen, die am elektronischen Identitätsnachweisverfahren teilnehmen wollen.

Für die Verwaltung werden 13 Informationspflichten eingeführt.

Für Bürgerinnen und Bürger werden vier Informationspflichten eingeführt. Hierdurch entsteht jeweils Aufwand in Höhe von 2 bis 10 Minuten. Wenn Bürgerinnen und Bürger den elektronischen Identitätsnachweis zu Hause am PC nutzen wollen, fallen einmalig Kosten in Höhe von 15 Euro für die Beschaffung des Kartenlesegerätes an. Die erforderliche Software wird kostenlos als Download zur Verfügung gestellt.

Für einen Antrag auf Reaktivierung des gesperrten elektronischen Identitätsnachweises muss der Antragsteller bzw. die Antragstellerin persönlich bei der Ausweisbehörde erscheinen. Hierdurch entstehen zusätzlich zu den beiden Behördengängen für die Antragstellung und die Abholung des Ausweises durch einen weiteren Behördengang Warte- und Wegezeiten.

Der Rat bittet daher das Ressort zu prüfen, ob mittelfristig auf zumindest einen der Behördengänge verzichtet werden kann. Denkbar wäre es zum Beispiel, die Ausweise den Bürgerinnen und Bürgern zuzuschicken. Ein solches Verfahren wurde im Rahmen eines Pilotprojekts der Stadt Freiburg im Breisgau im Jahr 2008 bereits getestet. Um die dagegen vorgebrachten Sicherheitsbedenken des Ressorts aufzugreifen, wäre es u. a. denkbar, die Ausweise nicht per einfacher Briefpost, sondern durch einen spezialisierten Lieferdienst zu verteilen. Ein derartiges Modell wird derzeit innerhalb der Projektgruppe

„Deutschland-Online Kfz-Wesen“ unter Federführung der Freien und Hansestadt Hamburg bzgl. der Auslieferung relevanter Dokumente der Zulassung von Kraftfahrzeugen untersucht.

Im Weiteren hat der Nationale Normenkontrollrat im Rahmen seines gesetzlichen Prüfauftrages keine Bedenken gegen das Regelungsvorhaben.

Dr. Ludewig	Bachmaier
Vorsitzender	Berichterstatter