

Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)

PAuswV

Ausfertigungsdatum: 01.11.2010

Vollzitat:

"Personalausweisverordnung vom 1. November 2010 (BGBl. I S. 1460), die zuletzt durch Artikel 2 der Verordnung vom 12. April 2024 (BGBl. 2024 I Nr. 125) geändert worden ist"

Stand: Zuletzt geändert durch Art. 2 V v. 12.4.2024 I Nr. 125

Fußnote

(+++ Textnachweis ab: 1.11.2010 +++)

Überschrift: IdF d. Art. 2 Nr. 1 V v. 15.10.2020 I 2199 mWv 1.1.2021

Eingangsformel

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 des Lichtbilds durch Dienstleister
Kapitel 3	Übermittlung der Ausweisantragsdaten
Kapitel 4	Produktion des Personalausweises
Kapitel 5	Ausgabe und Versand des Personalausweises; Braille-Aufkleber
Kapitel 6	Änderung von Daten des Personalausweises; nachträgliches Einschalten
Kapitel 7	Elektronischer Identitätsnachweis mit einem mobilen Endgerät
Kapitel 8	Sperrung und Entsperrung des elektronischen Identitätsnachweises
Kapitel 9	Beantragung von Berechtigungen
Kapitel 10	Ausgabe von Berechtigungszertifikaten
Kapitel 11	eID-Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums
Kapitel 12	Schlussvorschriften
Anhang 1	Muster des Personalausweises
Anhang 1a	Muster des Aufklebers zur Anschriftenänderung des Personalausweises
Anhang 1b	Muster des Aufklebers zur Anschriftenänderung des Personalausweises nach elektronischer Anmeldung nach § 23a des Bundesmeldegesetzes
Anhang 1c	Muster des Aufklebers mit Brailleschrift für den Personalausweis und die eID-Karte
Anhang 2	Muster des vorläufigen Personalausweises
Anhang 2a	Muster des Ersatz-Personalausweises
Anhang 3	Formale Anforderungen an die Einträge im Personalausweis

Anhang 3a	Muster der eID-Karte
Anhang 4	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 Dokumente (XhD) ist ein in erweiterbarer Seitenbeschreibungssprache (XML) verfasstes Datenaustauschformat für hoheitliche Dokumente.

(7) OSCI-Transport ist der vom Kooperationsausschuss Automatisierte Datenverarbeitung 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 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,
 - b) den Zugriffsschutz auf die im Chip des Personalausweises abgelegten Daten,
 - c) den Zugriffsschutz auf die in dem Chip eines mobilen Endgeräts abgelegten Daten sowie
2. die technischen und organisatorischen Anforderungen an
 - a) die Erfassung, Echtheitsbewertung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke,
 - b) die Übermittlung sämtlicher Ausweisantragsdaten und die in § 8 Absatz 1 Satz 2 genannten Daten von den Personalausweisbehörden an den Ausweishersteller,
 - c) den elektronischen Identitätsnachweis und das Vor-Ort-Auslesen,
 - 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,
 - e) das Zurücksetzen und Neusetzen der Geheimnummer durch den Ausweishersteller nach elektronisch gestelltem Antrag und

- f) das Ändern der Anschrift auf dem Personalausweis unter Verwendung eines Aufklebers nach Anhang 1 sowie auf dem Chip des Personalausweises nach einer elektronischen Anmeldung nach § 23a des Bundesmeldegesetzes,
- g) die Übermittlung der Daten nach § 10a Absatz 1 Satz 1 des Personalausweisgesetzes,
- h) den elektronischen Identitätsnachweis mit einem mobilen Endgerät und
- i) das sichere Verfahren der Übermittlung von Lichtbildern von einem Dienstleister an eine Personalausweisbehörde.

Der Stand der Technik ist als niedergelegt zu vermuten in den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik. Die Übersicht über die Technischen Richtlinien wird im Bundesanzeiger veröffentlicht; die jeweils geltende Fassung der Technischen Richtlinien wird im Bundesanzeiger durch Verweis auf die Internetseite des Bundesamtes für Sicherheit in der Informationstechnik bekannt gemacht.

§ 3 Zertifizierung von Systemkomponenten

(1) Aus Anhang 4 ergeben sich die Systemkomponenten

- 1. der Personalausweisbehörden,
- 2. des Ausweisherstellers,
- 3. der Cloudanbieter,
- 4. der Dienstleister, die Lichtbildaufnahmegeräte im Sinne des § 5a Absatz 2 Nummer 2 verwenden,
- 5. der Diensteanbieter und ihrer Auftragsverarbeiter nach Artikel 4 Nummer 8 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35), deren jeweilige Zertifizierung verpflichtend oder optional ist.

Die Art und die Einzelheiten der Zertifizierung sind den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zu entnehmen.

(2) Für die Zertifizierung gelten § 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist, sowie die BSI-Zertifizierungs- und Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231), die durch Artikel 40 des Gesetzes vom 29. März 2017 (BGBl. I S. 626) geändert worden ist, in der jeweils geltenden Fassung.

(3) Die Kosten der Zertifizierung trägt der Antragsteller.

§ 4 Dokumentationspflichten

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

- 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 Einschaltung des elektronischen Identitätsnachweises mit Datum und Uhrzeit der Einschaltung sowie die Personalausweisbehörde, die den elektronischen Identitätsnachweis eingeschaltet hat;
- 5. den Sperrantrag durch den Ausweisinhaber, die Übermittlung der Sperrsumme an den Sperrlistenbetreiber sowie das Datum und die Uhrzeit von Antrag und Übermittlung;
- 6. 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;
2. im Zusammenhang mit der Entsperrung des elektronischen Identitätsnachweises eines Personalausweises
 - 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 sowie
3. im Zusammenhang mit der Löschung des Sperreintrags des elektronischen Identitätsnachweises nach § 10 Absatz 8 Satz 1 des Personalausweisgesetzes
 - a) die Sperrsumme sowie das Datum und die Uhrzeit der Löschung,
 - 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.

(4) Der Cloudanbieter dokumentiert zum Zwecke der Nachverfolgbarkeit des Übermittlungsvorgangs eines erstellten und übermittelten Lichtbilds

1. die Übermittlung eines verschlüsselten Lichtbilds durch einen Dienstleister, das Datum und die Uhrzeit der Übermittlung sowie
2. den Abruf eines verschlüsselten Lichtbilds durch die Personalausweisbehörde sowie das Datum und die Uhrzeit des Abrufs.

§ 5 Speicherung und Löschung

(1) Für die Speicherung personenbezogener Daten nach dieser Verordnung bei den Personalausweisbehörden gilt § 23 Absatz 4 des Personalausweisgesetzes entsprechend. Lichtbilder, die nach § 6a durch Lichtbildaufnahmegeräte der Personalausweisbehörde gefertigt wurden, sind unverzüglich nach Abruf durch die Personalausweisbehörde von dem Lichtbildaufnahmegerät zu löschen.

(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 sowie der letzte Tag der Gültigkeitsdauer eines elektronischen Identitätsnachweises mit einem Personalausweis sind spätestens einen Monat nach Ablauf der Gültigkeitsdauer aus der Referenzliste zu löschen;
2. Sperrschlüssel und Sperrsumme sowie der letzte Tag der Gültigkeitsdauer eines elektronischen Identitätsnachweises mit einem mobilen Endgerät sind spätestens einen Monat nach Ablauf der Gültigkeitsdauer aus der Referenzliste zu löschen;
3. Aktualisierungen der Sperrliste werden gespeichert, damit eine Sperrung oder Entsperrung von elektronischen Identitätsnachweisen nachgewiesen werden kann; solche Aktualisierungen der

Sperrliste werden spätestens einen Monat nach Ablauf der Gültigkeitsdauer eines elektronischen Identitätsnachweises gelöscht;

4. ein allgemeines Sperrmerkmal wird aus der Sperrliste spätestens einen Monat nach Ablauf der Gültigkeitsdauer eines elektronischen Identitätsnachweises entfernt oder wenn die Personalausweisbehörde eine Entsperrung vorgenommen hat;
5. die nach § 4 Absatz 3 erzeugten Protokolldaten werden 20 Wochen nach ihrer Erzeugung gelöscht.

(4) Der Ausweishersteller speichert die Daten, die im Rahmen des Produktionsverfahrens erlangt oder erzeugt worden sind und der antragstellenden Person zugeordnet werden können, höchstens aber 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 sowie den jeweiligen letzten Tag der Gültigkeitsdauer von hergestellten Personalausweisen sowie von eingerichteten elektronischen Identitätsnachweisen mit einem mobilen Endgerät. Die Sperrsummen sowie der jeweilige letzte Tag der Gültigkeitsdauer von hergestellten Personalausweisen in dieser Liste sind spätestens einen Monat nach Ablauf der Gültigkeitsdauer eines elektronischen Identitätsnachweises zu löschen. Der Sperrlistenbetreiber informiert hierzu den Ausweishersteller über Löschvorgänge nach Absatz 3 Nummer 1 und 2. § 26 Absatz 3 Satz 1 des Personalausweisgesetzes bleibt unberührt. Die Sperrsummen sowie der letzte Tag der Gültigkeitsdauer eines elektronischen Identitätsnachweises mit einem mobilen Endgerät in dieser Liste sind spätestens einen Monat nach Ablauf der Gültigkeitsdauer zu löschen.

(5) Der Ausweishersteller löscht die zur Bearbeitung von elektronischen Anträgen nach § 20 Absatz 2 und § 21 Absatz 2 zu erhebenden personenbezogenen Daten, sobald er die Benachrichtigung bekommen hat, dass der Antragsteller die zufällig neu generierte Geheimnummer erhalten hat, spätestens aber nach 30 Tagen. Satz 1 gilt nicht für das dienste- und kartenspezifische Kennzeichen, welches spätestens nach 90 Tagen zu löschen ist.

(6) Abgesehen von der im Personalausweisregister zu speichernden Anschrift löscht die Personalausweisbehörde alle personenbezogenen Daten, die zur Änderung der Anschrift nach einer elektronischen Anmeldung nach § 23a des Bundesmeldegesetzes erhoben werden, nach Vollzug der Änderung der Anschrift auf dem Chip sowie Erstellung und Versand des Aufklebers, spätestens aber 30 Tage nach Erhalt der personenbezogenen Daten durch die Personalausweisbehörde.

(7) Der Cloudanbieter ist verpflichtet, das Lichtbild unverzüglich nach Abruf durch die Personalausweisbehörde, spätestens aber sechs Monate nach Empfang des Lichtbilds von einem Dienstleister, zu löschen, es sei denn, die Personalausweisbehörde hat auf Veranlassung der antragstellenden Person vermerkt, dass das Lichtbild für einen Zeitraum von höchstens sechs Monaten ab Antragstellung nicht gelöscht werden soll. Im Übrigen ist der Cloudanbieter verpflichtet, die bei ihm gespeicherten Daten für folgende Fristen zu speichern; nach Fristablauf sind die Daten zu löschen:

1. die Protokolldaten nach § 4 Absatz 4 für zehn Jahre und sechs Monate nach ihrer Erstellung;
2. die personenbezogenen Daten der Dienstleister sowie die diesen Personen zuzuordnenden Pseudonyme für sechs Monate, ab dem Zeitpunkt, ab dem der Kontoinhaber von dem Cloudanbieter die Auflösung seines Nutzerkontos verlangt hat;
3. abweichend von Nummer 2 die dort genannten Daten für zehn Jahre und sechs Monate seit der Übermittlung des Lichtbilds an die zuständige Personalausweisbehörde, wenn dieses für die Personalausweisbeantragung durch eine dem Nutzerkonto zuzuordnende Person übermittelt wurde.

Kapitel 2

Übermittlung des Lichtbilds durch Dienstleister

§ 5a Fertigung und Übermittlung des Lichtbilds durch ein sicheres Verfahren

(1) In Fällen, in denen ein Personalausweis bei einer Personalausweisbehörde nach § 8 Absatz 1 des Personalausweisgesetzes beantragt wird, kann die antragstellende Person einen Dienstleister mit der Fertigung des Lichtbilds beauftragen. Der Dienstleister hat das Lichtbild elektronisch zu fertigen und im Anschluss durch ein sicheres Verfahren an die Personalausweisbehörde zu übermitteln. Dienstleister ist jede natürliche oder juristische Person, die gewerbsmäßig Lichtbilder von anderen Personen anfertigt, die zur Vorlage bei einer Personalausweisbehörde bestimmt sind.

(2) Ein sicheres Verfahren im Sinne des Absatzes 1 Satz 2 ist:

1. die Übermittlung des Lichtbilds an die Personalausweisbehörde von einem Dienstleister unter Einbindung eines Cloudanbieters oder
2. die Übermittlung des Lichtbilds an die Personalausweisbehörde von einem zertifizierten Lichtbildaufnahmegerät eines Dienstleisters, das unmittelbar an das Behördennetz einer Personalausweisbehörde angeschlossen ist.

§ 5b Übermittlung des Lichtbilds unter Einbindung eines Cloudanbieters

- (1) Bei einer Übermittlung nach § 5a Absatz 2 Nummer 1 übermittelt der Dienstleister das Lichtbild an einen Cloudanbieter und übergibt der antragstellenden Person anschließend einen Code, den diese im Rahmen der Antragstellung der Personalausweisbehörde übergibt.
- (2) Mit diesem Code ruft die Personalausweisbehörde das Lichtbild bei dem Cloudanbieter ab. Durch den Abruf wird das Lichtbild gemeinsam mit dem Pseudonym des Dienstleisters an die Personalausweisbehörde übermittelt.
- (3) Die Übermittlung des Lichtbilds vom Dienstleister an die Personalausweisbehörde erfolgt verschlüsselt als Ende-zu-Ende-Verschlüsselung; eine Entschlüsselung durch den Cloudanbieter ist auszuschließen. Eine Übermittlung des Lichtbilds vom Dienstleister zum Cloudanbieter ist nur unter Verwendung von zertifizierten Komponenten nach Maßgabe von § 3 Absatz 1 Satz 1 zulässig.
- (4) Die Verarbeitung der personenbezogenen Daten darf ausschließlich durch einen im Gebiet der Europäischen Union ansässigen Cloudanbieter und ausschließlich im Gebiet der Europäischen Union erfolgen.

§ 5c Registrierung und Identifizierung eines Dienstleisters bei einem Cloudanbieter

- (1) Dienstleister haben sich bei einem Cloudanbieter mit einem Nutzerkonto zu registrieren. Bei der Registrierung ist ein Nachweis über die Dienstleistereigenschaft sowie ein Nachweis über die Identität des Dienstleisters zu erbringen.
- (2) Der Nachweis über die Dienstleistereigenschaft ist zu erbringen durch Übermittlung:
 1. eines Nachweises über die Gewerbebeanmeldung;
 2. durch einen Auszug aus dem Unternehmensregister;
 3. durch eine Bescheinigung der Mitgliedschaft in der Handwerkskammer oder
 4. einer Bestätigung eines Finanzamtes über die Anmeldung einer freiberuflichen Tätigkeit als Fotografin oder Fotograf.
- (3) Bei der Registrierung erfolgt der Nachweis der Identität des Dienstleisters durch
 1. einen elektronischen Identitätsnachweis gemäß § 18 des Personalausweisgesetzes, gemäß § 12 des eID-Karte-Gesetzes oder gemäß § 78 Absatz 5 des Aufenthaltsgesetzes oder
 2. ein anderes elektronisches Identifizierungsmittel, das nach Artikel 6 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44) auf dem Sicherheitsniveau „hoch“ im Sinne des Artikels 8 Absatz 2 Buchstabe c der Verordnung (EU) Nr. 910/2014 notifiziert worden ist.

Einem Nutzerkonto können mehrere Personen zugeordnet werden, wenn diese vom Dienstleister auf Dauer angelegt beschäftigt werden. Personen nach Satz 2 müssen sich bei der Registrierung in einem Nutzerkonto ebenfalls mittels eines der in Satz 1 genannten Identifizierungsmittel in dem Nutzerkonto registrieren.

- (4) Für jede Person, die sich in einem Nutzerkonto nach Absatz 3 registriert hat, wird durch den Cloudanbieter ein Pseudonym erzeugt.
- (5) Vor jeder Übermittlung eines Lichtbilds an den Cloudanbieter hat sich die übermittelnde Person des Dienstleisters erneut mit einem der in Absatz 3 Satz 1 genannten Identifizierungsmittel zu identifizieren. Bei jeder Übermittlung wird das Lichtbild durch den Cloudanbieter mit dem Pseudonym der übermittelnden Person dauerhaft verbunden. Die Personalausweisbehörde trägt im Personalausweisregister als lichtbildaufnehmende Stelle gemäß § 23 Absatz 3 Nummer 20 des Personalausweisgesetzes das übermittelte Pseudonym ein.

§ 5d Pflichten des Cloudanbieters

Wenn bestimmte Tatsachen die Annahme begründen, dass ein beim Cloudanbieter abgerufenes Lichtbild auf unzulässige Weise erstellt worden ist, kann die Personalausweisbehörde vom Cloudanbieter verlangen, Auskunft darüber zu geben, welcher Person das mit dem Lichtbild verbundene Pseudonym zuzuordnen ist. Dies gilt auch für den Fall, dass ein Cloudanbieter seinen Betrieb einstellt und solange, bis die Daten durch den Cloudanbieter gelöscht werden.

§ 5e Übermittlung des Lichtbilds von einem Lichtbildaufnahmegerät eines Dienstleisters

(1) Bei einer Übermittlung nach § 5a Absatz 2 Nummer 2 fertigt der Dienstleister das Lichtbild durch sein Lichtbildaufnahmegerät an, das mit Zustimmung der jeweiligen Personalausweisbehörde unmittelbar an ihr Behördenetzwerk angeschlossen ist.

(2) Mit dem Lichtbild wird der Name des Dienstleisters, der das Lichtbildaufnahmegerät zur Verfügung gestellt hat, sowie die Kennung des verwendeten Lichtbildaufnahmegeräts der Personalausweisbehörde übermittelt. Die Personalausweisbehörde trägt im Personalausweisregister als lichtbildaufnehmende Stelle gemäß § 23 Absatz 3 Nummer 20 des Personalausweisgesetzes den Namen des Dienstleisters und die Kennung des verwendeten Lichtbildaufnahmegeräts ein.

Kapitel 3 Übermittlung der Ausweisanztragsdaten

§ 6 Erfassung der Anschrift

Der Wohnort in der Anschrift nach § 5 Absatz 2 Nummer 9 Alternative 1 des Personalausweisgesetzes ist mit der amtlichen 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. Wird als Wohnort eine ausländische Anschrift glaubhaft gemacht, wird diese aufgenommen. Hierbei können die Besonderheiten der ausländischen Anschrift berücksichtigt werden, soweit diese technisch darstellbar sind und eine eindeutige Zuordnung der Anschrift ermöglichen.

§ 6a Fertigung des Lichtbilds durch die Personalausweisbehörde

(1) Wird das Lichtbild von der Personalausweisbehörde mit einem eigenen Lichtbildaufnahmegerät gefertigt, trägt die Personalausweisbehörde im Personalausweisregister als lichtbildaufnehmende Stelle gemäß § 23 Absatz 3 Nummer 20 des Personalausweisgesetzes die Personalausweisbehörde ein. Die Anfertigung des Lichtbilds mit einem eigenen Lichtbildaufnahmegerät ist nur zulässig, wenn das Lichtbildaufnahmegerät als Systemkomponente im Sinne des § 3 Absatz 1 Satz 1 zertifiziert worden ist.

(2) Das nach Absatz 1 gefertigte Lichtbild ist unverzüglich durch die Personalausweisbehörde vom Lichtbildaufnahmegerät zu löschen, wenn es durch die Personalausweisbehörde abgerufen wurde. Wird das gefertigte Lichtbild nicht sofort durch die Personalausweisbehörde abgerufen, so ist dieses bis zum Abruf zu speichern, längstens jedoch für 96 Stunden nach dessen Anfertigung.

§ 7 Qualitätssicherung des Lichtbildes und der Fingerabdrücke

(1) Ein Lichtbild, das nach § 9 Absatz 3 Satz 3 des Personalausweisgesetzes gefertigt wird, muss aktuell sein und den Vorgaben der Technischen Richtlinie TR-03121 des Bundesamts für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung entsprechen.

(2) Abweichend von Absatz 1 kann für einen Personalausweis, der im Ausland bei der Personalausweisbehörde nach § 8 Absatz 2 Personalausweisgesetz beantragt wird, auch ein aktuelles Lichtbild in der Größe von 45 Millimeter x 35 Millimeter im Hochformat und ohne Rand vorgelegt werden, sofern die elektronische Fertigung mittels Geräten der Behörde zur Lichtbildaufnahme nicht möglich ist.

(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 technischen Eigenschaften der gespeicherten Daten,
2. die Behördenkennzahl sowie
3. anonymisierte Protokolldaten zur Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke.

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 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 DeutschlandOnline-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 Personalausweisbehörden, Ausweishersteller und Vermittlungsstellen alle für eine elektronische und automatisierte Kommunikation benötigten technischen Verbindungsparameter im Deutschen Verwaltungsdienstverzeichnis (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 Verwaltungsdienstverzeichnis (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, für Bau und Heimat, dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundeskriminalamt zur Verfügung.

Kapitel 4 Produktion des Personalausweises

§ 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.

§ 12a Muster für den Ersatz-Personalausweis

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

§ 13 Schnittstelle des Chips

Der Chip 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 Chip 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) an den Chip übermittelt werden müssen,
2. Zugriffsrechte über Berechtigungszertifikate nachgewiesen werden müssen und
3. alle personenbezogenen Daten zwischen dem Chip und Inhabern von Berechtigungszertifikaten verschlüsselt übermittelt werden.

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

1. Behörden, die ein hoheitliches Berechtigungszertifikat nutzen,
2. berechtigte Diensteanbieter, die ein Berechtigungszertifikat nutzen, nach Eingabe der Geheimnummer durch den Ausweisinhaber, oder
3. berechtigte Vor-Ort-Diensteanbieter, die ein Vor-Ort-Zertifikat nutzen, nach Übermittlung der Zugangsnummer an den Chip.

§ 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, des Sperrschlüssels und des letzten Tages der Gültigkeitsdauer an den Sperrlistenbetreiber

Der Ausweishersteller übermittelt dem Sperrlistenbetreiber auf sicherem elektronischem Weg verschlüsselt und signiert die Sperrsumme, den Sperrschlüssel und den letzten Tag der Gültigkeitsdauer 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, den Sperrschlüssel und den letzten Tag der Gültigkeitsdauer übermittelt hat, keine Bestätigung erhalten, fragt er bei dem Sperrlistenbetreiber nach.

§ 17 Erhalt der Geheimnummer und der Entsperrnummer

(1) Die antragstellende Person erhält von der Personalausweisbehörde die Geheimnummer und die Entsperrnummer des Personalausweises in einem geschlossenen Kuvert. Dessen Erhalt hat die antragstellende Person in Textform zu bestätigen.

(2) Hat die antragstellende Person einen Wohnsitz oder ihren gewöhnlichen Aufenthalt außerhalb der Bundesrepublik Deutschland, können die Geheimnummer und die Entsperrnummer in einem Brief von der Personalausweisbehörde an die von der antragstellenden Person benannte Anschrift versandt werden, sofern die Aushändigung nicht bei Antragstellung erfolgen kann und die Abholung des Briefes bei der Personalausweisbehörde für die antragstellende Person nur unter unzumutbaren Umständen möglich wäre und der Wohnort in einem Staat liegt, in dem eine hinreichende Gewähr für eine ordnungsgemäße Übergabe auf dem Postweg besteht. Personalausweis und Geheimnummer dürfen nicht zusammen in einer Postsendung versandt werden. Bei als unzustellbar zurückgesandten Briefen erhält die antragstellende Person die Briefe von der Personalausweisbehörde nach Maßgabe von Absatz 1.

(3) Bis die antragstellende Person die Geheimnummer und die Entsperrnummer erhalten hat, gewährleistet die Personalausweisbehörde, dass Dritte keine Kenntnisnahme der Geheimnummer und der Entsperrnummer erhalten können.

Kapitel 5

Ausgabe und Versand des Personalausweises; Braille-Aufkleber

§ 18 Ausgabe und Versand des Personalausweises und des Sperrkennworts

(1) Der Personalausweis wird gemeinsam mit dem Sperrkennwort von der Personalausweisbehörde an die antragstellende Person, an eine andere nach § 9 Absatz 1 oder 2 des Personalausweisgesetzes berechnigte Person oder an eine von der antragstellenden Person bevollmächtigte Person ausgegeben.

(2) Der Personalausweis wird gemeinsam mit dem Sperrkennwort durch den Ausweishersteller an die zustellfähige inländische Meldeadresse der antragstellenden Person versendet, wenn sie einen gültigen Lichtbildausweis einer Behörde oder einer öffentlich-rechtlichen Körperschaft besitzt, der eine einwandfreie Feststellung ihrer Identität zulässt, und sie gegenüber der Personalausweisbehörde im Inland in dieses Verfahren eingewilligt hat. Ein Versand nach Satz 1 ist ausgeschlossen, wenn keine zustellfähige inländische Meldeadresse vorhanden ist. Der bisherige Personalausweis ist bei der Beantragung zu entwerten. Der Zusteller hat vor der Übergabe die Identität der antragstellenden Person durch Vorlage eines in Satz 1 genannten Lichtbildausweises zu überprüfen. Der Ausweishersteller informiert die Personalausweisbehörde über die erfolgte Übergabe des Personalausweises und des Sperrkennworts an die antragstellende Person.

(3) Die antragstellende Person soll bei einem Verfahren nach Absatz 2 der Personalausweisbehörde eine E-Mail-Adresse mitteilen, sofern eine solche der Personalausweisbehörde noch nicht vorliegt. Die Personalausweisbehörde übermittelt diese E-Mail-Adresse an den Ausweishersteller, damit dieser die E-Mail-Adresse dem Zusteller übermittelt. Der Zusteller kündigt in diesem Fall der antragstellenden Person den Zeitraum der Übergabe per E-Mail an die hinterlegte E-Mail-Adresse an. Die Ankündigung darf ausschließlich die Anrede, den Hinweis auf die bevorstehende Zustellung des Personalausweises, den voraussichtlichen Zustellzeitpunkt sowie die Modalitäten der Zustellung nach Absatz 2 Satz 4 enthalten. Die E-Mail-Adresse darf nur für die Zwecke verwendet werden, für die sie gespeichert wurde, und ist bei der Personalausweisbehörde, beim Ausweishersteller und beim Zusteller unverzüglich nach der Übergabe des Personalausweises an die antragstellende Person zu löschen, sofern sie ausschließlich für das Verfahren nach Absatz 2 gespeichert wurde. Erfolgt eine Übergabe nicht, so findet Satz 5 mit der Maßgabe Anwendung, dass der Ausweishersteller und der Zusteller die E-Mail-Adresse unverzüglich nach der Hinterlegung des Personalausweises bei der zuständigen Personalausweisbehörde, die Personalausweisbehörde diese unverzüglich nach der Ausgabe des Personalausweises an die antragstellende Person zu löschen haben.

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

(5) Für das Lesen der Daten nach Absatz 4 sind zertifizierte Lesegeräte mit hoheitlichem Berechnigungszertifikat zu verwenden.

(6) Abweichend von Absatz 2 darf die Personalausweisbehörde im Ausland Personalausweise gemeinsam mit dem Sperrkennwort auch auf dem Postweg versenden, ohne dass der Zusteller die antragstellende Person identifiziert, sofern die Abholung des Personalausweises für die antragstellende Person nur unter unzumutbaren

Umständen möglich wäre und der Wohnort in einem Staat liegt, in dem eine hinreichende Gewähr für eine ordnungsgemäße Übergabe besteht. Als unzustellbar zurückgesandte Personalausweise und Sperrkennwörter gibt die Personalausweisbehörde nach Maßgabe von Absatz 1 an die antragstellende Person aus.

(7) Wurde gegenüber der antragstellenden Person, die keine Wohnung in der Bundesrepublik Deutschland hat, eine Anordnung nach § 6 Absatz 7 des Personalausweisgesetzes getroffen, soll die Ausgabe des Personalausweises durch die Personalausweisbehörde in Deutschland erfolgen, in deren Bezirk die antragstellende Person für ihre Wohnung, bei mehreren Wohnungen für ihre Hauptwohnung, zuletzt meldepflichtig war. War die antragstellende Person noch nie in der Bundesrepublik Deutschland meldepflichtig, soll die Ausgabe durch eine von der antragstellenden Person zu benennende Personalausweisbehörde in der Bundesrepublik Deutschland erfolgen. Die Ausgabe des Personalausweises an eine andere nach § 9 Absatz 1 oder 2 des Personalausweisgesetzes berechnigte Person oder an eine von der antragstellenden Person bevollmächtigte Person ist in diesen Fällen ausgeschlossen.

§ 18a Aufkleber mit Brailleschrift

Auf Antrag des Ausweisinhabers wird durch die Personalausweisbehörde entweder bei Ausgabe des Personalausweises oder zu einem späteren Zeitpunkt ein Aufkleber mit Brailleschrift nach Anhang 1a auf dem Personalausweis angebracht.

Kapitel 6

Änderung von Daten des Personalausweises; nachträgliches Einschalten

§ 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. Hat der Ausweisinhaber eine elektronische Anmeldung nach § 23a des Bundesmeldegesetzes durchgeführt, wird nach erfolgter Änderung der Anschrift nach Absatz 2 Satz 4 ein Aufkleber nach Anhang 1b mit der neuen Anschrift durch die Personalausweisbehörde auf dem Postweg an die Zuzugsanschrift der antragstellenden Person versendet. Der Ausweisinhaber hat den Aufkleber unverzüglich auf dem Ausweis auf dem für die Anschrift vorgesehenen Feld anzubringen.

(2) Die Personalausweisbehörde ändert die auf dem Chip gespeicherte Anschrift. Hat der Ausweisinhaber eine elektronische Anmeldung nach § 23a des Bundesmeldegesetzes durchgeführt, hat er die Änderung der Anschrift auf dem Chip einzuleiten. Hierzu wird durch die Personalausweisbehörde ein elektronisches Formular bereitgestellt. Der Ausweisinhaber weist seine Identität gegenüber der Personalausweisbehörde mit einem elektronischen Identitätsnachweis nach § 18 Absatz 2 Satz 1 Nummer 1 des Personalausweisgesetzes nach. Die zuständige Personalausweisbehörde ändert die Anschrift auf dem Chip des Personalausweises und trägt diese in das Personalausweisregister ein. Ist die zuständige Personalausweisbehörde nicht die ausstellende Personalausweisbehörde, informiert die zuständige Personalausweisbehörde die ausstellende Personalausweisbehörde über die neue Anschrift und letztere ändert das Personalausweisregister.

(3) Für die Änderung der Daten nach Absatz 2 Satz 1 sind zertifizierte Geräte mit hoheitlichem Berechnigungszertifikat zu verwenden. Für den elektronischen Identitätsnachweis nach Absatz 2 Satz 3 sowie für das Ändern der Daten nach Absatz 2 Satz 4 verwendet die Personalausweisbehörde ein hoheitliches Berechnigungszertifikat.

(4) Die Personalausweisbehörde ändert die Anschrift im Ersatz-Personalausweis in den dafür vorgesehenen Datenfeldern.

§ 20 Neusetzung und Änderung der Geheimnummer für den elektronischen Identitätsnachweis mit dem Personalausweis

(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) Ein Ausweisinhaber, der eine Meldeadresse im Inland hat, kann das Neusetzen der Geheimnummer auch durch Verwendung der Zugangsnummer und eines hierfür vom Ausweishersteller zur Verfügung gestellten

elektronischen Formulars beantragen. Der Ausweishersteller schaltet die Funktion zum elektronischen Identitätsnachweis ab und versendet eine neue, zufällig generierte Geheimnummer in einem Brief an die im Chip gespeicherte Anschrift des Ausweisinhabers. Bei der Übergabe ist die Identität des Ausweisinhabers durch den Zusteller durch Vorlage des Personalausweises zu überprüfen. Nach Erhalt der neuen Geheimnummer meldet sich der Ausweisinhaber erneut beim Ausweishersteller unter Verwendung der Zugangsnummer an. Der Ausweishersteller schaltet die Funktion zum elektronischen Identitätsnachweis wieder ein und schreibt die neue, zufällig generierte Geheimnummer in den Chip. Der Ausweisinhaber ändert die neue, zufällig generierte Geheimnummer in eine selbst gewählte Geheimnummer.

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

(4) Für die Änderung der Daten nach Absatz 1 Satz 1 sind zertifizierte Geräte mit hoheitlichem Berechtigungszertifikat zu verwenden. Für das Ändern der Daten nach Absatz 2 Satz 2 sowie für das Einschalten nach Absatz 2 Satz 5 verwendet der Ausweishersteller ein hoheitliches Berechtigungszertifikat.

§ 21 Nachträgliches Einschalten

(1) Bevor die ausstellende oder zuständige Personalausweisbehörde einen ausgeschalteten elektronischen Identitätsnachweis nach § 10 Absatz 3 des Personalausweisgesetzes einschaltet, prüft sie die Identität des Ausweisinhabers. Die Personalausweisbehörde löscht die Tatsache der Ausschaltung im Personalausweisregister. Handelt die zuständige Personalausweisbehörde, informiert sie die ausstellende Personalausweisbehörde über die Einschaltung; in diesem Fall löscht die ausstellende Personalausweisbehörde die Tatsache der Ausschaltung im Personalausweisregister. 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.

(2) Der Antrag nach § 10 Absatz 3 des Personalausweisgesetzes kann durch den Ausweisinhaber, der eine Meldeadresse im Inland hat, auch durch Verwendung der Zugangsnummer und eines hierfür vom Ausweishersteller zur Verfügung gestellten elektronischen Formulars gestellt werden. Der Ausweishersteller versendet eine neue, zufällig generierte Geheimnummer in einem Brief an die im Chip gespeicherte Anschrift des Ausweisinhabers. Bei der Übergabe ist die Identität des Ausweisinhabers durch den Zusteller durch Vorlage des Personalausweises zu überprüfen. Nach Erhalt der neuen Geheimnummer meldet sich der Ausweisinhaber erneut beim Ausweishersteller unter Verwendung der Zugangsnummer an. Der Ausweishersteller schaltet die Funktion zum elektronischen Identitätsnachweis ein und schreibt die neue, zufällig generierte Geheimnummer in den Chip. Der Ausweisinhaber ändert die neue, zufällig generierte Geheimnummer in eine selbst gewählte Geheimnummer.

(3) Für das nachträgliche Einschalten des elektronischen Identitätsnachweises nach Absatz 1 sind zertifizierte Geräte mit hoheitlichem Berechtigungszertifikat zu verwenden. Für das Ändern der Daten nach Absatz 2 Satz 2 sowie für das Einschalten nach Absatz 2 Satz 5 verwendet der Ausweishersteller ein hoheitliches Berechtigungszertifikat.

Kapitel 7

Elektronischer Identitätsnachweis mit einem mobilen Endgerät

§ 22 Einrichtung

(1) Der Ausweisinhaber leitet die Einrichtung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät durch Verwendung eines elektronischen Formulars ein.

(2) Der Ausweishersteller prüft, ob das mobile Endgerät über einen zugelassenen Chip verfügt, welcher dem Stand der Technik entspricht.

(3) Der Ausweisinhaber führt gegenüber dem Ausweishersteller einen elektronischen Identitätsnachweis nach § 18 Absatz 2 Satz 1 Nummer 1 des Personalausweisgesetzes durch.

(4) Der Ausweishersteller übermittelt in einem sicheren Verfahren, welches dem Stand der Technik entspricht, die Daten nach § 5 Absatz 5a des Personalausweisgesetzes auf den Chip des mobilen Endgeräts. Hierzu verwendet er ein hoheitliches Berechtigungszertifikat.

(5) Der Ausweisinhaber vergibt eine selbstgewählte, sechsstellige Geheimnummer durch zweimalige, übereinstimmende Eingabe.

(6) Der Ausweishersteller

1. erzeugt das Sperrkennwort, welches dem Ausweisinhaber über die verwendete Software angezeigt wird,
2. übermittelt den letzten Tag der Gültigkeitsdauer, die Sperrsumme und den Sperrschlüssel an den Sperrlistenbetreiber,
3. speichert das dienste- und kartenspezifische Kennzeichen jeweils für den Chip des Personalausweises und des mobilen Endgeräts sowie das Datum und die Uhrzeit der Einrichtung des elektronischen Identitätsnachweises, den letzten Tag der Gültigkeitsdauer, den Hersteller und die Modellbezeichnung des mobilen Endgeräts, die Sperrsumme und das Sperrkennwort und
4. versendet einen einfachen Brief an die im Chip des Personalausweises gespeicherte Anschrift des Ausweisinhabers, in dem das Datum und die Uhrzeit der Einrichtung des elektronischen Identitätsnachweises, der letzte Tag der Gültigkeitsdauer, das Sperrkennwort und der Hersteller und die Modellbezeichnung des mobilen Endgeräts mitgeteilt wird; der Brief enthält ferner Angaben zur Erreichbarkeit des Sperrdienstes.

(7) Der Hersteller eines nach Absatz 1 zu verwendenden elektronischen Formulars hat den Ausweisinhaber darauf hinzuweisen, dass das mobile Endgerät hinsichtlich der auf seinem Chip nach Absatz 1 gespeicherten Daten mit besonderer Sorgfalt zu behandeln ist. Der Inhalt des Hinweistextes ist von dem Hersteller einer nach Absatz 1 verwendeten Software mit dem Bundesministerium des Innern, für Bau und Heimat abzustimmen.

§ 23 Speicherung von personenbezogenen Daten; Zugriffsschutz

Auf einen elektronischen Identitätsnachweis mit einem mobilen Endgerät sind § 14 Absatz 1 mit der Maßgabe, dass abweichend von § 14 Absatz 1 Nummer 1 vor der Übermittlung personenbezogener Daten stets die Geheimnummer übermittelt werden muss, sowie § 14 Absatz 2 Nummer 1 und 2 entsprechend anzuwenden.

§ 23a Neusetzen und Änderung der Geheimnummer für den elektronischen Identitätsnachweis mit einem mobilen Endgerät

(1) Kennt der Ausweisinhaber die bei der Einrichtung des elektronischen Identitätsnachweises mit einem mobilen Endgerät vergebene Geheimnummer nicht, kann ein neuer Antrag nach § 10a Absatz 1 Satz 1 des Personalausweisgesetzes gestellt werden.

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

§ 23b Gültigkeitsdauer

Der elektronische Identitätsnachweis mit einem mobilen Endgerät hat eine Gültigkeitsdauer von zwei Jahren.

Kapitel 8

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 mit dem Personalausweis

(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. 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.

§ 25a Sperrung des elektronischen Identitätsnachweises mit einem mobilen Endgerät

(1) Kommt ein mobiles Endgerät, auf welches Daten nach § 10a Absatz 1 Satz 1 des Personalausweisgesetzes übermittelt wurden, abhanden, hat der Ausweisinhaber den elektronischen Identitätsnachweis über den Sperrnotruf unverzüglich sperren zu lassen. Der Sperrnotruf hat den Ausweisinhaber vor der Sperrung zu identifizieren.

(2) Der Sperrnotruf erzeugt unverzüglich die Sperrsumme und übermittelt sie unverzüglich dem Sperrlistenbetreiber.

(3) Der Sperrlistenbetreiber hat den Eintrag des allgemeinen Sperrmerkmals in die Sperrliste unverzüglich gegenüber dem Sperrnotruf zu bestätigen.

§ 26 Entsperrung des elektronischen Identitätsnachweises mit dem Personalausweis

(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.

§ 26a Entsperrung des elektronischen Identitätsnachweises mit mobilem Endgerät

Anstelle einer Entsperrung eines gesperrten elektronischen Identitätsnachweises mit einem mobilen Endgerät kann ein erneuter Antrag nach § 10a Absatz 1 Satz 1 des Personalausweisgesetzes gestellt werden.

§ 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 mit dem Personalausweis oder einem mobilen Endgerät 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 9 Beantragung von Berechtigungen

§ 28 Antrag auf Erteilung einer Berechtigung für Vor-Ort-Diensteanbieter und sonstige Diensteanbieter

(1) Der Antrag auf Erteilung einer Berechtigung nach § 21 Absatz 2 des Personalausweisgesetzes oder der Antrag auf Erteilung einer Vor-Ort-Berechtigung nach § 21a des Personalausweisgesetzes muss folgende Angaben enthalten:

1. Angaben, die zur Feststellung der Identität von juristischen und natürlichen Personen notwendig sind,
 - a) bei natürlichen Personen insbesondere der Familienname, die Vornamen, der Tag und der Ort der Geburt sowie die Anschrift der Hauptwohnung,
 - b) bei juristischen Personen insbesondere der Name, die Anschrift des Sitzes, die Rechtsform und die Bevollmächtigten; außerdem ist in diesem Fall eine Kopie des Handelsregisterauszugs oder der Errichtungsurkunde beizufügen;
2. Kontaktdaten, insbesondere die telefonische oder elektronische Erreichbarkeit;
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 kurze Beschreibung des Diensteanbieters und seiner Tätigkeitsfelder sowie die Angabe der Unternehmenswebsite, soweit vorhanden;
5. eine kurze Beschreibung des dem Antrag zu Grunde liegenden Interesses an einer Berechtigung; darzulegen ist, welche Funktion
 - a) im Falle eines Antrages auf Erteilung einer Berechtigung nach § 21 Absatz 2 des Personalausweisgesetzes der elektronische Identitätsnachweis oder
 - b) im Falle eines Antrages auf Erteilung einer Vor-Ort-Berechtigung nach § 21a des Personalausweisgesetzes das Vor-Ort-Auslesenim Rahmen der behördlichen Aufgabenwahrnehmung oder der vorgesehenen Geschäftszwecke der antragstellenden Person erfüllen soll;
6. die Angabe der Datenkategorien nach § 18 Absatz 3 des Personalausweisgesetzes, auf die die antragstellende Person zugreifen möchte;
7. die Erklärung, dass der Diensteanbieter den betrieblichen Datenschutz einhält;
8. die Angabe, ob die antragstellende Person sich zur Durchführung des elektronischen Identitätsnachweises eines Auftragnehmers nach den Artikeln 28 bis 31 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) bedienen wird und in diesem Fall 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 bedarf der Schriftform.

§ 29 Antrag auf Erteilung einer Berechtigung für Identifizierungsdiensteanbieter; Vorgaben zu Datenschutz und Datensicherheit bei Identifizierungsdiensteanbietern

(1) Für den Antrag auf Erteilung einer Berechtigung für Identifizierungsdiensteanbieter nach § 21b des Personalausweisgesetzes gilt § 28 entsprechend.

(2) Die nach § 21b Absatz 2 Satz 1 Nummer 1 des Personalausweisgesetzes einzuhaltenden technisch-organisatorischen Maßnahmen und die weiteren Anforderungen an die Datensicherheit nach § 21 Absatz 2 Satz 1 Nummer 2 des Personalausweisgesetzes legt das Bundesamt für Sicherheit in der Informationstechnik im Benehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in einer Technischen Richtlinie fest. Dies umfasst insbesondere Anforderungen an die Datenspeicherung und -löschung, das einzusetzende Verschlüsselungsverfahren sowie an das Informationssicherheitsmanagement.

(3) Die Einhaltung der in Absatz 2 genannten Voraussetzungen hat der Antragsteller durch Vorlage eines Zertifikats des Bundesamtes für Sicherheit in der Informationstechnik nachzuweisen. Das Bundesamt für Sicherheit in der Informationstechnik darf sich bei seiner Überprüfung externer Dienstleister bedienen. Die hierbei anfallenden Kosten trägt der Antragsteller.

(4) Die weiteren Anforderungen an den Datenschutz nach § 21b Absatz 2 Satz 1 Nummer 2 des Personalausweisgesetzes liegen nicht vor, wenn

1. der Staat des Wohnsitzes oder des Sitzes der antragstellenden Person kein angemessenes Datenschutzniveau gewährleistet entsprechend der Verordnung (EU) 2016/679,
2. der elektronische Identitätsnachweis für den Identifizierungsdiensteanbieter durch einen Auftragnehmer nach den Artikeln 28 bis 31 der Verordnung (EU) 2016/679 durchgeführt wird und hierbei kein wirksames Auftragsverhältnis nach den Artikeln 28 bis 31 der Verordnung (EU) 2016/679 zwischen dem Diensteanbieter und dem Auftragnehmer besteht,
3. der Identifizierungsdiensteanbieter einen Auftragnehmer nach den Artikeln 28 bis 31 der Verordnung (EU) 2016/679 gewählt hat, der die technischen und organisatorischen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik für die sichere Bereitstellung des elektronischen Identitätsnachweises nicht erfüllt,
4. der Identifizierungsdiensteanbieter nicht die Voraussetzungen des § 21 Absatz 2 des Personalausweisgesetzes erfüllt.

§ 29a Einholung von Stellungnahmen der Datenschutzaufsichtsbehörden

Die Vergabestelle für Berechtigungszertifikate kann jederzeit eine Stellungnahme der zuständigen Datenschutzaufsichtsbehörde einholen, ob dort Umstände bekannt sind, aus denen sich Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung ergeben. Vor Erteilung der Berechtigung soll die Vergabestelle die Stellungnahme der Datenschutzaufsichtsbehörde nur in Zweifelsfällen abwarten.

§ 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 10

Ausgabe von Berechtigungszertifikaten

§ 31 Angaben vor der Ausgabe von Berechtigungszertifikaten

Berechtigungszertifikateanbieter dürfen Berechtigungszertifikate für den elektronischen Identitätsnachweis bereitstellen, wenn sie vor Aufnahme dieser Tätigkeit gegenüber der Vergabestelle für Berechtigungszertifikate 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 jeweils geltende Fassung wird im Bundesanzeiger durch Verweis auf die Internetseite des Bundesamtes für Sicherheit in der Informationstechnik bekannt gemacht.

§ 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 § 20a Absatz 1 des Personalausweisgesetzes dürfen vorbehaltlich von Satz 2 ausschließlich an die zur Identitätsfeststellung berechtigten Behörden ausgegeben werden. Zum Zwecke der Qualitätssicherung anhand von Testausweisen dürfen hoheitliche Berechtigungszertifikate auch an das Bundesamt für Sicherheit in der Informationstechnik ausgegeben werden.

(2) Das Bundesministerium des Innern, für Bau und Heimat bestimmt, welche Stellen hoheitliche Berechtigungszertifikate an welche zur Identitätsfeststellung berechtigten Behörden ausgeben dürfen, und veröffentlicht dies im 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 berechnete Stellen dokumentieren Empfänger, zugrunde liegende Berechtigung sowie das Datum und die Uhrzeit der Ausgabe von Berechtigungszertifikaten.

§ 36a Ausgabe von Berechtigungszertifikaten für öffentliche Stellen anderer Mitgliedstaaten

Der Bund stellt Berechtigungszertifikate für öffentliche Stellen anderer Mitgliedstaaten zur Verfügung. Die Kommunikation und die Identifizierung der öffentlichen Stellen erfolgt über die einheitlichen Ansprechpartner nach dem Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung gemäß Artikel 12 Absatz 7 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 53 vom 25.2.2015, S. 14).

Kapitel 11

eID-Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums

§ 36b Entsprechende Anwendung der Vorschriften über den Personalausweis

(1) Soweit dieses Kapitel keine besonderen Regelungen enthält, gelten für die die eID-Karte betreffenden Angelegenheiten die Vorschriften des Kapitels 1 sowie der Kapitel 3 bis 10 entsprechend.

(2) An die Stelle von Ausweis und Ausweisinhaber treten die eID-Karte und ihr Inhaber, an die Stelle der Personalausweisbehörden treten die eID-Karte-Behörden, an die Stelle des Personalausweisregisters tritt das eID-Kartenregister.

§ 36c Nicht auf die eID-Karte entsprechend anwendbare Vorschriften

Auf die eID-Karte finden keine Anwendung:

1. § 2 Satz 1 Nummer 1 Buchstabe a und Nummer 2 Buchstabe a,

2. § 4 Absatz 1 Nummer 4,
3. § 7,
4. § 8 Absatz 1 Satz 2 Nummer 3,
5. § 9,
6. § 11,
7. § 12,
8. § 12a,
9. § 19 Absatz 1 und 4 sowie
10. § 21.

§ 36d Abweichende Regelung für die eID-Karte

§ 20 Absatz 2 Satz 3 gilt mit der Maßgabe, dass der Zusteller bei der Übergabe des Briefes die Identität der antragstellenden Person durch Vorlage eines Personalausweises oder Passes des Mitgliedstaates, dessen Staatsangehörigkeit die antragstellende Person besitzt, zu überprüfen hat.

§ 36e Muster der eID-Karte

Die eID-Karte ist nach dem in Anhang 3a abgedruckten Muster herzustellen. Für die einzutragenden Daten gelten die formalen Anforderungen des Anhangs 3 Abschnitt 1 entsprechend.

Kapitel 12 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.

(3) Abweichend von § 19 Absatz 1 Satz 1 können die Personalausweisbehörden der Länder, die nach § 23a des Bundesmeldegesetzes ein Verfahren zur elektronischen Anmeldung erproben, bis zum 30. April 2022 auch Änderungsaufkleber nach dem in Anhang 1a abgedruckten Muster verwenden.

(4) Bis zum Ablauf des 31. Dezember 2032 gilt § 5 Absatz 3 Nummer 1, 3 und 4 sowie Absatz 4 Satz 4 mit den Maßgaben, dass die Frist zehn Jahre und drei Monate beträgt und wie folgt zu laufen beginnt:

1. im Fall von § 5 Absatz 3 Nummer 1 mit der Eintragung in die Referenzliste,
2. im Fall von § 5 Absatz 3 Nummer 3 mit der Speicherung der Aktualisierung der Sperrliste,
3. im Fall von § 5 Absatz 3 Nummer 4 mit der Speicherung des Sperrschlüssels beim Sperrlistenbetreiber oder mit der Entsperrung durch die Personalausweisbehörde,
4. im Fall von § 5 Absatz 4 Satz 4 mit der Eintragung der Sperrsummen oder des jeweils letzten Tages der Gültigkeitsdauer von hergestellten Personalausweisen in dieser Liste.

(5) Bis zum 31. Oktober 2024 findet § 17 Absatz 1 und 2 mit der Maßgabe Anwendung, dass das Kuvert neben der Geheimnummer und der Entsperrnummer das Sperrkennwort enthalten kann, wenn dieses der antragstellenden Person von dem Ausweishersteller übersandt wird. Als Absenderanschrift ist die postalische Anschrift der ausstellenden Personalausweisbehörde anzugeben. Der Erhalt des Kuverts ist in diesem Fall unmittelbar vor der Aushändigung des Personalausweises und in der Form nach § 17 Absatz 1 Satz 2 durch die antragstellende Person zu bestätigen.

§ 38 Inkrafttreten

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

Schlussformel

Der Bundesrat hat zugestimmt.

Anhang 1 Muster des Personalausweises

(Fundstelle: BGBl. 2024 I Nr. 125)

Vorderseite



Rückseite



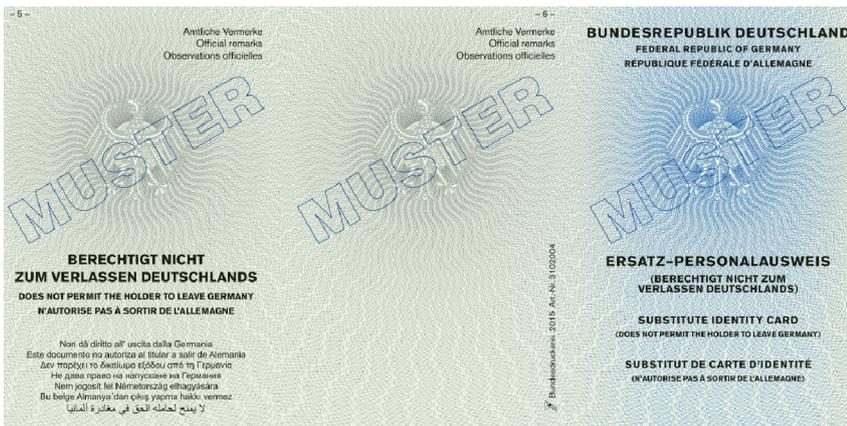
Muster des Aufklebers zur Anschriftenänderung des vorläufigen Personalausweises



Anhang 2a Muster des Ersatz-Personalausweises

(Fundstelle: BGBl. I 2015, 1102)

Vorderseite



Rückseite



Anhang 3

(Fundstelle: BGBl. I 2010, 1471 - 1474;
bzgl. der einzelnen Änderungen vgl. Fußnote)

Abschnitt 1

Formale Anforderungen an die Einträge in Ausweisen im Sinne des § 2 Absatz 1 des Personalausweisgesetzes

Vorbemerkung:

1. Die in der nachstehenden Tabelle beschriebenen Anforderungen an die Einträge gelten sowohl für den Personalausweis als auch für den vorläufigen Personalausweis und den Ersatz-Personalausweis.
2. Die Personalausweisbehörden verwenden zur Personalisierung der vorläufigen Personalausweise und der Aufkleber zur Anschriftenänderung sowie zur Personalisierung der Ersatz-Personalausweise und zur Änderung von Daten der Ersatz-Personalausweise den Schriftfont „UnicodeDoc“. Hierfür sind Tintenstrahldrucker einzusetzen. Die Tinte hat die nach der ISO 1831:1980-10 geforderten Eigenschaften hinsichtlich maschineller Lesbarkeit im B900-Band zu erfüllen. Es ist ausschließlich solches Schreibmaterial zu verwenden, das nach DIN ISO 12757-1:1999-02 urkunden- und kopierecht ist.
3. Als Zeichensatz ist der in der jeweils gültigen Fassung der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik, BSI: Technische Richtlinie TR-03123, XML-Datenaustauschformat für hoheitliche Dokumente (TR XhD), veröffentlichte Zeichensatz „String.Latin“ zu verwenden.
4. Der maschinenlesbare Bereich in den Ausweisen ist im Schriftfont OCR-B zu beschriften.

5. In den Datenfeldern „Name“ (Familiename und Geburtsname) sowie „Vornamen“ sind alle Namensbestandteile komplett darzustellen, soweit dies technisch entsprechend der nachstehenden Tabelle umsetzbar ist.
6. Grundsätzlich sind alle Einträge in den Ausweisen in der Schriftgröße 1 gemäß der nachstehenden Tabelle vorzunehmen.
Wird in einem Datenfeld die zur Verfügung stehende Zeichenzahl in der Schriftgröße 1 überschritten, sind sämtliche Zeichen des entsprechenden Datenfeldes in Schriftgröße 2 einzutragen.
Sollte auch unter Ausnutzung der Schriftgröße 2 die nach Maßgabe der nachstehenden Tabelle maximal zur Verfügung stehende Zeichenzahl nicht ausreichen, sind die Einträge des Datenfeldes (zum Beispiel Vornamen) – unter Ausnutzung der maximal zur Verfügung stehenden Zeichenzahl – entsprechend gekürzt vorzunehmen.
Bei dem vorläufigen Personalausweis und bei dem Ersatz-Personalausweis ist im Datenfeld „Name“ der Eintrag gemäß den Vorgaben der nachstehenden Tabelle in der Schriftgröße 1 und 2 im Fettdruck zulässig. Einträge in den sonstigen Datenfeldern sind nur in der Schriftgröße 1 zulässig. Sollte unter Ausnutzung dieser Schriftgrößen die zur Verfügung stehende Zeichenzahl nicht ausreichen, sind die Einträge des Datenfeldes (zum Beispiel Vornamen) entsprechend gekürzt vorzunehmen.
Unterschiedliche Schriftgrößen innerhalb eines Datenfeldes sind unzulässig.
Bei der Personalisierung des Aufklebers zur Änderung der Anschrift auf dem Personalausweis ist die Seriennummer in der Schriftgröße 3 einzutragen. Die Eintragungen zur Postleitzahl, zum Wohnort sowie zur Straße und Hausnummer sind in der Schriftgröße 3 im Fettsatz vorzunehmen.
7. Sofern neben dem Familiennamen auch ein Geburtsname vorhanden ist, ist der Geburtsname in einer eigenen Zeile einzutragen. Bei vorläufigen Personalausweisen und Ersatz-Personalausweisen ist dem Geburtsnamen die Zeichenfolge „GEB.“ unter Hinzufügung eines Leerzeichens voranzustellen.
8. Soweit ein oder mehrere Doktorgrade vorhanden sind, wird dieser bzw. werden diese im Personalausweis im Datenfeld „Doktorgrad“, im vorläufigen Personalausweis im Datenfeld „Name“ eingetragen. Die Anzahl der für den Namenseintrag vorgesehenen Zeichen verringert sich um die für die Eintragung des Doktorgrades bzw. der Doktorgrade benötigte Zeichenzahl, sofern diese Eintragung im Datenfeld „Name“ vorgenommen wird.
9. Die alphanummerische Seriennummer des Personalausweises wird ausschließlich aus den Buchstaben C, F, G, H, J, K, L, M, N, P, R, T, V, W, X, Y, Z und den Ziffern 1, 2, 3, 4, 5, 6, 7, 8, 9 gebildet. Beim vorläufigen Personalausweis und beim Ersatz-Personalausweis besteht die Seriennummer aus einem Buchstaben und sieben Ziffern.
10. Das Lichtbild, das von der antragstellenden Person in den Abmaßen 35 x 45 mm vorzulegen ist, ist bei der Personalisierung im vorläufigen Personalausweis verkleinert mit den Abmessungen 29 x 37 mm darzustellen.

Datenfelder	Anzahl der zur Verfügung stehenden Zeichen	
	Schriftgröße ¹ 1 Schriftfont des Ausweisherstellers: (2 mm) UnicodeDoc: 2,4 mm	Schriftgröße 2 Schriftfont des Ausweisherstellers: (1,3 mm) UnicodeDoc: 2 mm
Name (Familiename und Geburtsname)	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)	Einträge in Schriftgröße 2 sind unzulässig
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)	Einträge in Schriftgröße 2 sind unzulässig

Datenfelder	Anzahl der zur Verfügung stehenden Zeichen	
	Schriftgröße ¹ 1 Schriftfont des Ausweisherstellers: (2 mm) UnicodeDoc: 2,4 mm	Schriftgröße 2 Schriftfont des Ausweisherstellers: (1,3 mm) UnicodeDoc: 2 mm
Gültig bis (letzter Tag der Gültigkeitsdauer)	10 Zeichen pro Zeile; 1 Zeile (insgesamt 10 Zeichen)	Einträge in Schriftgröße 2 sind unzulässig
Wohnort	25 Zeichen pro Zeile; 2 Zeilen (insgesamt 50 Zeichen)	Einträge in Schriftgröße 2 sind unzulässig
Straße und Hausnummer	25 Zeichen pro Zeile; 2 Zeilen (insgesamt 50 Zeichen)	Einträge in Schriftgröße 2 sind unzulässig
Größe	3 Zeichen pro Zeile; 1 Zeile (insgesamt 3 Zeichen)	Einträge in Schriftgröße 2 sind unzulässig
Farbe der Augen	19 Zeichen pro Zeile; 1 Zeile (insgesamt 19 Zeichen)	Einträge in Schriftgröße 2 sind unzulässig
Doktorgrad	20 Zeichen pro Zeile; 1 Zeile (insgesamt 20 Zeichen)	31 Zeichen pro Zeile; 1 Zeile (insgesamt 32 Zeichen)
Ordens- und Künstlernamen ²	20 Zeichen pro Zeile; 1 Zeile (insgesamt 20 Zeichen)	31 Zeichen pro Zeile; 1 Zeile (insgesamt 32 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 Zeile (insgesamt 8 Zeichen)	Einträge in Schriftgröße 2 sind unzulässig

¹ Die Schriftgröße ist am Großbuchstaben E auszurichten.

² Gilt nur für den Personalausweis.

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

Datenfelder des Aufklebers für Anschriftenänderungen nach elektronischer Anmeldung nach § 23a des Bundesmeldegesetzes	Anzahl der zur Verfügung stehenden Zeichen	
	Schriftgröße 3 UnicodeDoc: 1,5 mm	
Anschrift	22 Zeichen pro Zeile, 4 Zeilen (insgesamt 88 Zeichen)	
Seriennummer	9 Zeichen pro Zeile; 1 Zeile (insgesamt 9 Zeichen)	

Abschnitt 2

<p>Musterfoto</p> <p>Qualitativ hochwertige Fotos sind die Grundlage einer einwandfreien Wiedergabe des Bildes und Voraussetzung für die Anwendung der Gesichtsbio metrie 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. Die antragstellende 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.</p>	
<p>Format</p> <p>Das Foto muss die Gesichtszüge der Person von der Kinns spitze 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 Kinns spitze 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 Gesichtgröße zu verkleinern. Das Gesicht muss zentriert auf dem Foto platziert sein.</p>	
<p>Schärfe und Kontrast</p> <p>Das Gesicht muss in allen Bereichen scharf abgebildet, kontrastreich und klar sein.</p>	
<p>Ausleuchtung</p> <p>Das Gesicht muss gleichmäßig ausgeleuchtet werden. Reflexionen oder Schatten im Gesicht sowie rote Augen sind zu vermeiden.</p>	

<p>Hintergrund</p> <p>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.</p>	
<p>Fotoqualität</p> <p>Das Foto sollte mit einer Auflösung von mindestens 600 dpi vorliegen. Das Foto muss farbneutral sein und die natürlichen Hauttöne wiedergeben. Digitale Fotos sind grundsätzlich in Farbe vorzulegen. Ist die Vorlage eines papierbasierten Fotos in Ausnahmefällen gestattet, darf dieses Foto in Farbe oder Schwarzweiß vorgelegt werden; es darf jedoch keine Knicke oder Verunreinigung aufweisen.</p>	
<p>Kopfposition und Gesichtsausdruck</p> <p>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.</p>	
<p>Augen und Blickrichtung</p> <p>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.</p>	
<p>Brillenträger</p> <p>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.</p>	

<p>Kopfbedeckung</p> <p>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.</p>	
<p>Kinder</p> <p>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 Kinnschuppe bis zum oberen Kopfbereich. Dabei ist das obere Kopfbereich unter Vernachlässigung der Frisur anzunehmen. Wegen des häufig nicht eindeutig zu bestimmenden oberen Kopfbereiches 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.</p>	
<p>Säuglinge und Kleinkinder</p> <p>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.</p>	

Anhang 3a Muster der eID-Karte

(Fundstelle: BGBl. I 2020, 2200)

Vorderseite

[PDF-Dokument wird in eigenem Fenster angezeigt](#)

Rückseite

[PDF-Dokument wird in eigenem Fenster angezeigt](#)

Anhang 4 Übersicht über die zu zertifizierenden Systemkomponenten

(Fundstelle: BGBl. I 2010, 1476;
bzgl. der einzelnen Änderungen vgl. Fußnote)

Nr.	Bezeichnung der Systemkomponente	Verpflichtung/Option
1	Chip auf der Ausweiskarte (Hard- und Software)	Verpflichtung für den Ausweishersteller
2	Hardware zur Erfassung und Echtheitsbewertung von Fingerabdrücken	Verpflichtung für die Anbieter dieser Geräte Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden

Nr.	Bezeichnung der Systemkomponente	Verpflichtung/Option
3	Software zur Erfassung, Echtheitsbewertung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke	Verpflichtung für den Ausweishersteller Verpflichtung für die Personalausweisbehörden
4	(weggefallen)	
5	Erfassungsstation zur Fertigung des Lichtbildes	Verpflichtung für die Personalausweisbehörden, die das Lichtbild gemäß §§ 6a, 7 Absatz 1 Satz 3 selbst fertigen oder für Dienstleister, die Lichtbildaufnahmegeräte im Sinne des § 5a Absatz 2 Nummer 2 verwenden
6	Modul für die Datenübermittlung von den Personalausweisbehörden 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 Visualisierungsmodul 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.
10	eID-Client	Optionale Durchführung durch den Anbieter dieser Software. Empfehlung des Einsatzes zertifizierter Software an den Ausweisinhaber
11	Hard- und Software zur Durchführung des elektronischen Identitätsnachweises oder des Vor-Ort-Auslesens bei den Diensteanbietern oder ihrer Auftragnehmer (eID-Server)	Verpflichtung für den Diensteanbieter oder dessen Auftragnehmer
12	Hard- und Software zum Betrieb der Cloud	Verpflichtung für den Cloudanbieter
13	Software zur Verschlüsselung und Übertragung der Lichtbilder von Dienstleistern an die Cloud	Verpflichtung für die Softwarehersteller