

# Neuer Personalausweis

Aus der Praxis für die Praxis

Beantragung von Zertifikaten  
für das Auslesen von Daten aus  
dem neuen Personalausweis

Tina Siegfried  
Martin Riedel  
Lars Terbeck

Stand: April 2011

# Informationen zur Beantragung von Zertifikaten bei der Vergabestelle für Berechtigungszertifikate für das Auslesen von Daten aus dem neuen Personalausweis

---

Vitako, die Bundesarbeitsgemeinschaft der kommunalen IT-Dienstleister, hat in Kooperation mit der Stadt Hagen und der Datenzentrale Baden Württemberg sowie in Abstimmung mit der Vergabestelle für Berechtigungszertifikate (VfB) im Bundesverwaltungsamt Szenarien für den Einsatz des neuen Personalausweises in kommunalen Portalen entworfen.

Wir stellen hier Informationen zur Verfügung, die genutzt werden können, um entsprechende Zertifikate zu beantragen. Bei Übernahme der hier angebotenen Formulierungen geht die VfB von einer zügigen Verfahrensabwicklung aus, weil alle wichtigen Angaben vorhanden sind und Rückfragen kaum nötig sein werden.

Berlin, im April 2011

## Inhalt

1. Einleitung.....	3
2. Antragstellung.....	4
3. Geschäftszweck.....	4
4. Denkbare Szenarien.....	4
4.1 Anlegen und Nutzung eines Bürgerkontos zur Abwicklung von Online-Services.....	4
4.2 Anlegen eines temporären Bürgerkontos zur Nutzung kommunaler Online-Dienste.....	5
5. Beschreibung von Geschäftsprozessen.....	6
5.1 Registrierung Bürgerkonto.....	6
5.2 Temporäres Bürgerkonto.....	7
5.3 Login Bürgerkonto.....	8
6. Begründung von Datenkategorien.....	9
6.1 Zertifikat1: Bürgerkonto.....	9
6.2 Zertifikat 2: Temporäres Bürgerkonto.....	9
7. Einzureichende Unterlagen.....	10
7.1 Diensteanbieter.....	10
7.2 Ansprechpartner.....	11
7.3 Sonstiges.....	12
8. Nutzung von eID-Server oder eID-Service.....	13
9. Muster für eine Datenschutzerklärung.....	14

## 1. Einleitung

Kommunen stellen ihren Bürgern Informationen und Online-Services über ihre örtlichen Portale (meist unter [www.kommunenname.de](http://www.kommunenname.de)) zur Verfügung. Oft werden im Bereich Bürgerservice elektronische Dienste und/oder Formulare angeboten. Damit Bürger diese Services über das Internet (auch mehrfach) nutzen können, besteht seit November 2010 die Möglichkeit, sich mit dem neuen Personalausweis (nPA) mit aktivierter eID-Funktion (zur elektronischen Identifizierung) am Portal anzumelden.

Ein zentraler Vorteil des neuen Personalausweises besteht für Kommunen und ihre Online-Services darin, dass mit der eID-Funktion erstmals die zweifelsfreie Identifizierung eines Verwaltungskunden möglich wird. Damit besteht die Chance, dass die Services der Verwaltung für die Bürger und Unternehmen noch stärker auf deren Bedürfnisse ausgerichtet werden und sie schneller und effizienter abgewickelt werden können. Die eindeutige Identifizierung erleichtert den Zugang zu Online-Angeboten. Und die Übernahme von Kundendaten aus dem Ausweis direkt in ein Online-Formular spart Zeit auf beiden Seiten und verringert darüber hinaus die Gefahr von Eingabe- oder sonstigen Übertragungsfehlern.

Kommunen, die den nPA zur Identifizierung ihrer Bürger bei der Nutzung von Online-Services einsetzen wollen, müssen bei der Vergabestelle für Berechtigungszertifikate (VfB) eine Erlaubnis beantragen, aus der hervorgeht, welche personen- und ausweisbezogenen Daten sie aus dem Personalausweis auslesen wollen. Mit dieser Erlaubnis kann sich die Kommune das Berechtigungszertifikat bei einem Anbieter beschaffen. Nur Anbieter mit einem Berechtigungszertifikat können die beantragten Datenfelder aus den Ausweisen auslesen, wobei der Ausweisinhaber jederzeit die Kontrolle darüber behält, welche seiner Daten er an den Anbieter von Online-Diensten übermitteln will. Dies dient dem Schutz vor einem unberechtigten Auslesen der persönlichen Daten und bietet gleichzeitig den Vorteil, dass man sicher sein kann, dass das „Gegenüber“ im Internet tatsächlich der Anbieter ist, der er vorgibt zu sein. Um ein Zertifikat zu erhalten, müssen der Zweck der Datenerhebung und die Datenkategorien, die für den jeweiligen Dienst ausgelesen werden sollen, angegeben und begründet werden. Außerdem ist eine Darstellung der Geschäftsprozesse notwendig, für die Erlaubnisse beantragt werden.

Die Nutzung der eID-Funktion setzt außerdem eine funktionierende Infrastruktur voraus, wie z. B. die für Berechtigungszertifikate und das Sperrmanagement benötigte Public Key Infrastruktur, an der eine Reihe von Behörden und Institutionen beteiligt sind. Dazu gehören v.a. das Bundesamt für die Sicherheit in der Informationstechnik (BSI), die Vergabestelle für Berechtigungszertifikate sowie die Zertifikateanbieter, die die eigentliche technische Ausstellung der Berechtigungszertifikate übernehmen. Um den elektronischen Identitätsnachweis des neuen Personalausweises nutzen zu können, müssen sich Diensteanbieter an diese Infrastruktur anbinden. Dies kann auf mehreren Wegen geschehen. Wer keine aufwändige und teure Eigenentwicklung vornehmen will, kann die vom BSI bereits zertifizierten eID-Server nutzen und muss sich nicht selber um die Kommunikation zwischen der Software des Ausweisinhabers, dem Chip auf dem Personalausweis und um die Überprüfung von Berechtigungen und Prüfung gegen die Sperrliste kümmern. Möglich ist auch die Nutzung eines kompletten eID-Services, also die Beauftragung eines externen Dienstleisters, der für mehrere Dienste einen mandantenfähigen eID-Server betreibt.

## **2. Antragstellung**

Anträge auf die Erteilung einer Erlaubnis zum Auslesen von Daten aus dem neuen Personalausweis sind in der Regel Kommunen. Auch Landkreise oder Länder können Anträge stellen. Öffentliche IT-Dienstleister betreiben in der Regel im Auftrag ihrer Kommunen deren Onlinedienste (Auftragsdatenverarbeitung nach §11 BDSG). Der IT-Dienstleister selbst tritt aber nicht als Diensteanbieter in Erscheinung, sondern die Kommune. Es handelt sich hier also um eine Übermittlung von Daten an Dritte aus einem Verwaltungsauftrag und nicht um eine geschäftsmäßige Weitergabe von Daten, die nach §21 Abs.2 Nr. 2 PAuswG verboten ist.

In Nordrhein-Westfalen wird zurzeit geprüft, ob die IT-Dienstleister, die in der Form von Zweckverbänden nach dem Gesetz über Kommunale Gemeinschaftsarbeit Aufgaben ihrer Kommunen übertragen bekommen haben, auch als datenschutzrechtlich Verantwortliche gelten und dementsprechend dann ebenfalls Anträge stellen könnten.

## **3. Geschäftszweck**

Zweck der Datenerhebung (Geschäftszweck) ist die zweifelsfreie Identifizierung eines Bürgers für die medienbruchfreie Antragstellung über Online-Services. Dafür werden aus dem Personalausweis die Datenfelder Name, Vorname, Adresse und Geburtsdatum ausgelesen, weitere Informationen sind nicht erforderlich. Diese Angaben reichen aus, um den Bürger in jedem Fachverfahren eindeutig zu identifizieren. Auch in den Fällen, in denen aufgrund besonderer fachgesetzlicher Vorschriften eine zweifelsfreie Identifizierung notwendig ist (z.B. Gewerbeordnung, Jugendschutzgesetz etc.), kann diese mithilfe des elektronischen Identitätsnachweises durchgeführt werden.

## **4. Denkbare Szenarien**

Wir stellen hier zwei verschiedene Szenarien vor, bei denen der nPA für die Abwicklung elektronischer Bürgerdienste der Kommunen genutzt werden kann.

### **4.1 Anlegen und Nutzung eines Bürgerkontos zur Abwicklung von Online-Services**

Bürger können sich im kommunalen Portal ein sog. Bürgerkonto anlegen, bei dem sie sich bei wiederholter Nutzung entweder mit dem nPA oder optional mit einem weiteren Sicherheitsmerkmal wie z.B. Passwort authentifizieren. Das Bürgerkonto wird neuerdings auch als ID-Safe bezeichnet.

Der Vorteil einer solchen Lösung liegt auf der Hand: anstatt sich jedes Mal für einen Dienst zu registrieren, weist sich der Bürger nur einmal gegenüber dem Portal aus, seine Daten können nun für alle von ihm angeforderten Dienste genutzt werden, die Adresse und das Geburtsdatum z.B. müssen nicht immer wieder erneut händisch eingegeben werden, sondern werden automatisch in die entsprechenden Formulare übernommen. Weitere Möglichkeiten der Nutzung eines Bürgerkontos bestehen z.B. in der Online-Rechnungstellung durch die Kommune und der Zahlung per Lastschrift oder Kreditkarte durch den Bürger.

Der für die Beantragung des Zertifikats anzugebende **Zweck** in diesem Szenario lautet:

„Anlegen eines Bürgerkontos und Login in das Bürgerkonto. Der Bürger nutzt die eID-Funktion des nPA zur Bestätigung eines neu angelegten Bürgerkontos“

#### **4.2 Anlegen eines temporären Bürgerkontos zur Nutzung kommunaler Online-Dienste**

Bürger, die kein Bürgerkonto anlegen wollen, können sich temporär anmelden und ebenfalls mit Hilfe der eID-Funktion des neuen Personalausweises elektronische Dienste oder Formulare nutzen. In diesem Fall werden die benötigten Daten für jeden Verwaltungsvorgang nur temporär ausgelesen und nach Beendigung des Vorgangs gelöscht. Für solche Bürgerdienste ohne Registrierung wird ein weiteres Berechtigungszertifikat benötigt.

Der für die Beantragung des Zertifikats anzugebende **Zweck** in diesem Szenario lautet:

„Abwicklung von Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung (temporäres Bürgerkonto). Die vom Bürger freigegebenen Daten werden nicht gespeichert und nur temporär zur Abwicklung von Diensten verwendet“

Für beide Szenarien gilt: Sowohl die im Bürgerkonto hinterlegten Daten als auch die temporär aus dem Ausweis ausgelesenen Daten werden nur zum Zweck der Identifizierung des Bürgers durch die Verwaltung genutzt und können nicht mehr verändert werden. Die Daten werden darüber hinaus erst nach Zustimmung des Nutzers an das Fachverfahren weitergereicht (§ 13 Telemediengesetzes).

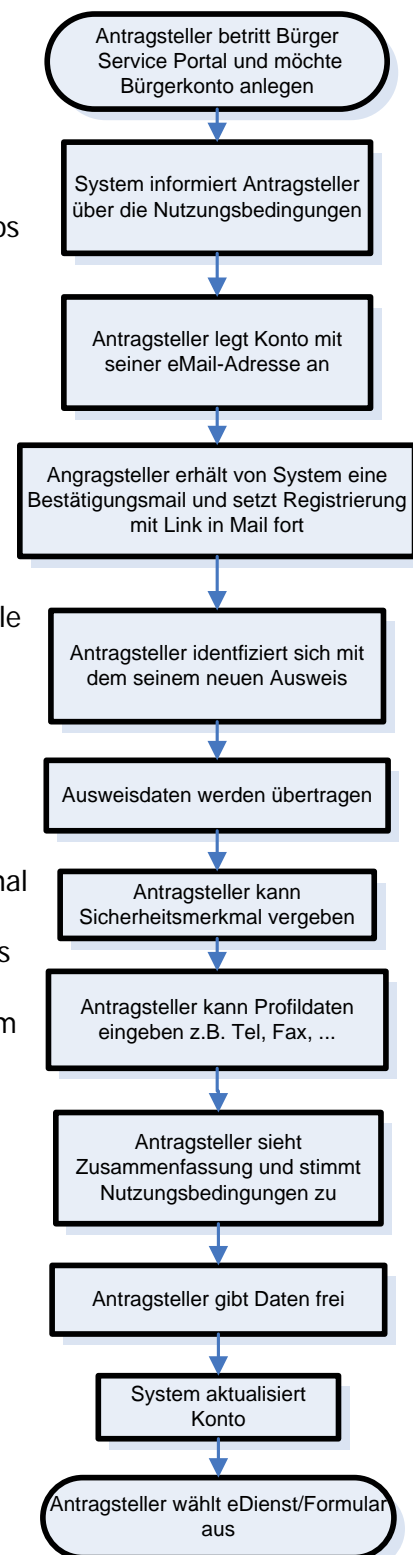
## 5. Beschreibung von Geschäftsprozessen

Die hier dargestellten Geschäftsprozesse sind exemplarisch und können an die eigenen Abläufe angepasst werden

### 5.1 Registrierung Bürgerkonto

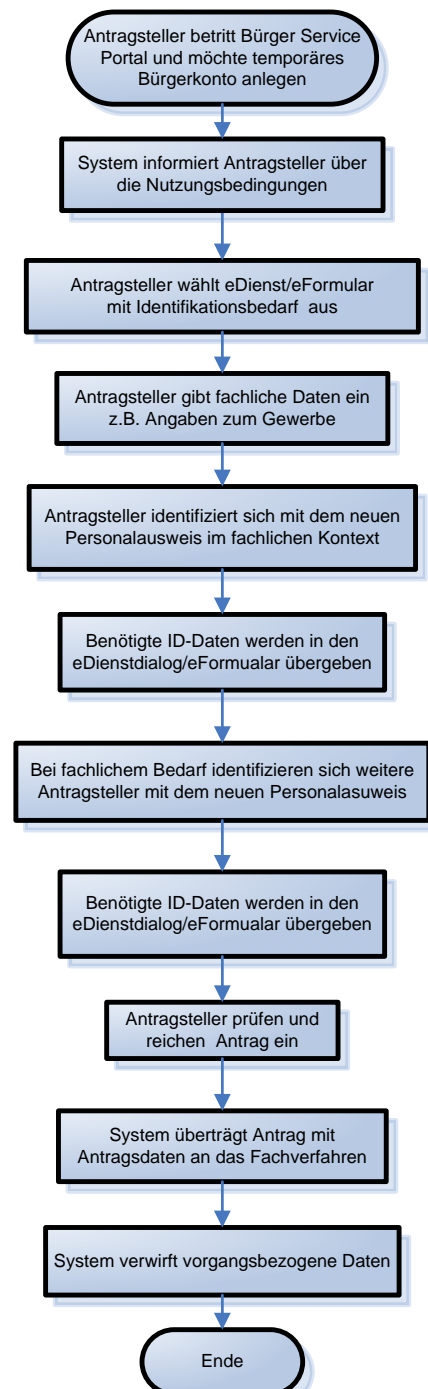
Der Antragsteller kann eine Dienstleistung mit Unterstützung seines Bürgerkontos abwickeln. Das Anlegen des Bürgerkontos erfolgt in mehreren Schritten. Im ersten Schritt legt er das Bürgerkonto mit seiner eMail-Adresse an. Der Bürger erhält daraufhin eine eMail zur Bestätigung des Bürgerkontos. Nach Abrufen der Mail zu einem späteren Zeitpunkt folgt der Antragsteller im nächsten Schritt dem Link in seiner Mail und bestätigt daraufhin die Identität mit seinem Ausweis. Die Ausweisdaten und die eingegebenen Profildaten werden nach Zustimmung des Antragstellers im eID-Safe gespeichert. Mit diesem Ablauf wird sichergestellt, dass die ID-Daten erst mit der Bestätigung einer gültigen eMail Adresse übernommen werden. Die eMail-Adresse wird für viele Anwendungsszenarien benötigt, z.B. für Benachrichtigungsmails in Verwaltungsvorgängen.

Der Registrierungsprozess erfordert mehrere Schritte, die teilweise asynchron ausgeführt werden, zum Beispiel eMail-Versand, und ist dem fachlichen Kontext daher unmittelbar vorgeschaltet. Zur alternativen Wiedererkennung des Kontos (z.B. bei Verlust des Ausweises) kann der Antragsteller optional ein weiteres Sicherheitsmerkmal, z.B. ein Passwort vergeben. In den Nutzungsbedingungen wird dem Bürger erläutert, dass er das Nutzerkonto nur zum Zweck von Bürgerdiensten und bei konkretem Anliegen einrichten darf. Die ID-Daten aus dem Bürgerkonto werden erst nach Zustimmung des Nutzers weitergegeben.



## 5.2 Temporäres Bürgerkonto

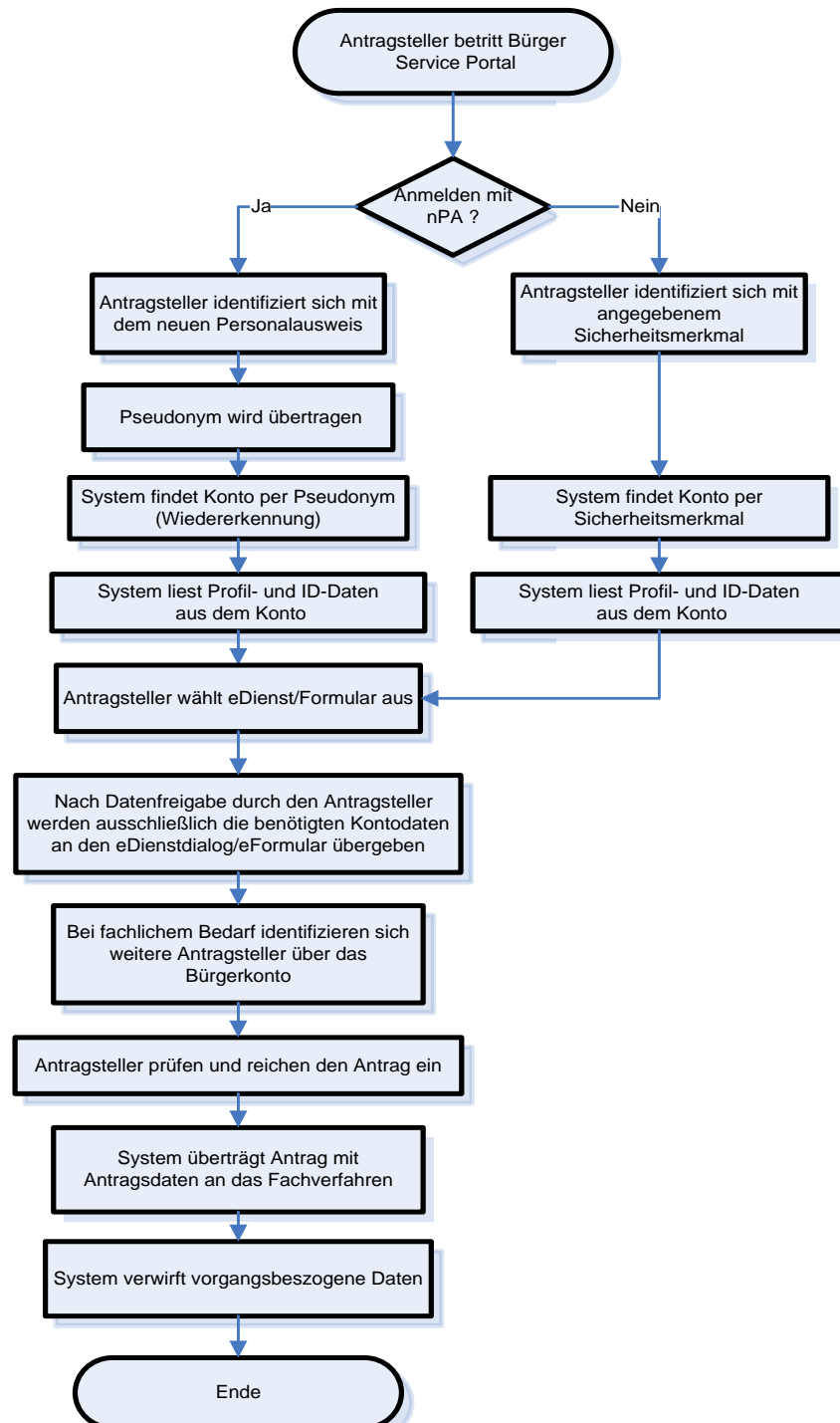
Das temporäre Bürgerkonto dient der Identifikation der Antragsteller zur Abwicklung von Verwaltungsdienstleistungen ohne Registrierung. Die Verwaltungsdienstleistungen werden in Form von eFormularen und eDiensten als Webanwendung über das Kommunalportal als Bürgerservice angeboten. Die Antragsteller weisen sich im fachlichen Kontext mit dem neuen Personalausweis aus. Durch Einreichen des Antrags überträgt das System ausschließlich die benötigten Daten an das Fachverfahren.





### 5.3 Login Bürgerkonto

Zur wiederholten Nutzung des Dienstes kann sich der Bürger mit dem Ausweis oder alternativ mit bei der Registrierung vergebenem Sicherheitsmerkmal anmelden. Die Anmeldung kann im Bürger Service Portal erfolgen oder im fachlichen Kontext der Anwendung.



## 6. Begründung von Datenkategorien

Die Datenkategorien werden für den angegebenen Geschäftszweck der zweifelsfreien Identifizierung als Bürger der Kommune X benötigt.

### 6.1 Zertifikat1: Bürgerkonto

#### Name, Vorname, Geburtsdatum, Anschrift

Diese Datengruppen werden für das bestätigte Bürgerkonto zur Nutzung in Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung erhoben. Die Daten werden bei der Erstanmeldung des Bürgers ausgelesen und im ID-Safe gespeichert.

#### Abkürzung „D“ für Bundesrepublik

Bei Verwaltungsdienstleistungen z.B. im Rahmen der EU-DLR muss das Land unterschieden werden. Diese Datengruppe wird bei der Erstanmeldung des Bürgers ausgelesen und im ID-Safe gespeichert.

#### Dokumentenart

Bei Verwaltungsdienstleistungen (z.B. im Ausländerwesen) muss unterschieden werden, ob ein nPA oder ein eAT vorliegt. Diese Datengruppe wird bei der Erstanmeldung des Bürgers ausgelesen und im ID-Safe gespeichert.

#### Dienste- und kartenspezifisches Kennzeichen (DKK):

Dieses Stammdatum wird bei der Erstanmeldung des Bürgers ausgelesen und im ID-Safe gespeichert.

Bei weiteren Anmeldungen wird es zur Wiedererkennung des Bürgers verwendet, um den Bürger zu identifizieren. Alternativ kann sich der Bürger mit dem Sicherheitsmerkmal anmelden. Der Bürger entscheidet, welche Anmeldequalität (nPA oder Sicherheitsmerkmal) er nutzen möchte. Die Kommune entscheidet, welche Dienste welche Anmeldequalität benötigen.

### 6.2 Zertifikat 2: Temporäres Bürgerkonto

#### Name, Vorname, Geburtsdatum, Anschrift

Diese Datengruppen werden in Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung erhoben.

#### Abkürzung „D“ für Bundesrepublik

Bei Verwaltungsdienstleistungen z.B. im Rahmen der EU-DLR muss das Land unterschieden werden. Diese Datengruppen werden in Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung erhoben.

#### Dokumentenart

Bei Verwaltungsdienstleistungen (z.B. im Ausländerwesen) muss unterschieden werden, ob ein nPA oder ein eAT vorliegt. Diese Datengruppen werden in Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung erhoben.

Diese Datengruppen werden nicht gespeichert.

## 7. Einzureichende Unterlagen

Die Formen und Voraussetzungen der Einreichung des Antrags bei der VFB sind unter folgender URL nachlesbar: [http://www.personalausweisportal.de/clin\\_102/DE/Partnerwerden/Anbieter/CVPS/cvps.html?nn=830936](http://www.personalausweisportal.de/clin_102/DE/Partnerwerden/Anbieter/CVPS/cvps.html?nn=830936)

Folgende Informationen sind für die Beantragung zu ermitteln und bereitzuhalten, es handelt sich hierbei um Pflichtfelder der Antragsapplikation bzw. Pflichtangaben bei schriftlicher oder persönlicher Beantragung:

### 7.1 Diensteanbieter

**7.1 Erstantrag**

**7.1.1 Angaben über den Antragsteller (Firma/Behörde)**

**Nachricht erstellen : Erstantrag**

Angaben über den Antragsteller (Firma / Behörde) | Ansprechpartner | Deutsche/r Vertreter/in | Sonstiges

**Diensteanbieter**

**Name: \* (150)**

**Name Kurz:**

**Geschäftsfeld:**

**Anschrift**

**Straße: \* (50)**

**Hausnr:**

**PLZ:**

**Ort: \* (50)**

**Bundesland:**

**Land: \* (50)**

**eMail / Rufnummern**

**eMail: \* (100)**

**Telefon: \* (50)**

**Fax:**

**Sonstiges**

**Sparte: \***

**Handelsregisternummer:**

- Name
- Kurzname
- Geschäftsfeld
- Anschrift
- E-Mail
- Telefon
- Telefax
- URL des Webauftritts

## 7.2 Ansprechpartner

**7.1.2 Ansprechpartner**

Nachricht erstellen : Erstantrag

Angaben über den Antragsteller (Firma / Behörde) | **Ansprechpartner** | Deutsche/r Vertreter/in | Sonstiges

**Name**

Anrede: +

Nachname: \* (50)

Vorname: \* (50)

Titel:

Zusatz:

**Anschrift**

Straße: \* (50)

Hausnr:

PLZ:

Ort: \* (50)

Land: \* (50)

**eMail / Rufnummern**

eMail: \* (100)

Telefon: \* (50)

Mobil:

Fax:

**Sonstiges**

Geburtsdatum: \* (tt.mm.jjjj)

Geburtsort: \* (50)

- Anrede
- Vorname
- Adresse
- E-Mail
- Telefon
- Fax
- Geburtsdatum
- Geburtsort

## 7.3 Sonstiges

### Datenschutzbeauftragter

The screenshot shows a web browser window with a form titled "7.1.4 Sonstiges" under the heading "Nachricht erstellen : Erstantrag". The form is divided into several sections:

- Angaben über den Antragsteller (Firma / Behörde):** Includes fields for "Name: \* (50)" and "eMail: \* (100)".
- Sonstiges:** Includes a dropdown menu for "Datenschutzaufsichtsbehörde: \*" and a text field for "Berechtigungszertifikatsanbieter / BerCA:".
- Anlagen:** Includes a section for "Fügen Sie bitte folgende Anlagen als PDF hinzu (maximale Größe je Dokument 500 KB):". It contains three items:
  - "Datenschutzerklärung: \*" with a "Durchsuchen..." button.
  - "Handelsregisterauszug: (nur für E-Business: \*)" with a "Bitte fügen Sie Ihren Handelsregisterauszug hinzu" label and a "Durchsuchen..." button.
  - "Nachweis der Erforderlichkeit der Datenfelder nach §18Abs.3 PAuswG: \*" with a "Durchsuchen..." button.
- Angaben zum eID-Service:** Includes a checkbox "Setzen Sie bitte hier einen Haken, falls Sie einen Technischen Dienstleister in Anspruch nehmen:" and a text field for "Technischer Dienstleister (Anlagen als PDF maximale Größe 500 KB):" with a "Durchsuchen..." button.

- Name
- E-Mail
- Datenschutzaufsichtsbehörde
- Datenschutzerklärung (PDF)

### Nachweis der Erforderlichkeit der Datenfelder

Nachweis der Erforderlichkeit der Datenfelder nach §18 Abs.3 PAuswG (PDF). Die aufgelisteten Datenfelder, die aus dem Personalausweis ausgelesen werden können, bedürfen einer nachvollziehbaren Begründung seitens des Diensteanbieters, wieso der Diensteanbieter für seinen Geschäftszweck welche Daten auslesen möchte. Beim Nachweis der Erforderlichkeit der Daten kann sich die Kommune auf die Vielzahl der Bundes- und Landesgesetze sowie die Ortssatzungen berufen.

## 8. Nutzung von eID-Server oder eID-Service

Der eID-Server stellt die Kommunikation zum Bürgerclient (AusweisApp) her und übernimmt die Kommunikation zum Abruf von Berechtigungszertifikaten und Sperrlisten. Dabei sind zwei Modelle hinsichtlich der Nutzung des eID-Servers vorstellbar. Einerseits kann der eID-Server lokal bei der Kommune betrieben werden oder als eID-Service von einem Dritten bezogen werden.

Die Entwicklung eines eigenen eID-Servers ist zertifizierungspflichtig. Beim Betrieb eines eID-Servers muss eine ISO-Zertifizierung vorliegen und er muss konform zu den technischen Richtlinien sein. Weitergehende Informationen sind über das Portal vom Bundesamt für Sicherheit in der Informationstechnik ([www.bsi.bund.de](http://www.bsi.bund.de)) zu erhalten.

Möchte die Behörde einen eigenen eID-Server betreiben, so muss sie die folgenden Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) erfüllen:

- Einsatz von Signaturkarten für alle privaten Schlüssel
- Einhaltung des Datenschutzes (z. B. Bundesdatenschutzgesetz)
- Erstellung eines Sicherheitskonzepts

Weitergehende Informationen sind über das Portal vom Bundesamt für Sicherheit in der Informationstechnik ([www.bsi.bund.de](http://www.bsi.bund.de)) zu erhalten.

Darüber hinaus empfiehlt das CompetenceCentrum neuer Personalausweis ein BSI IT-Grundschutzaudit nach dem Qualifizierungs- und Zertifizierungsschema des BSI.

Entscheidet sich eine Kommune den eID Service eines Dritten zu nutzen, so ist darauf zu achten, dass der eID-Server des Dritten die Anforderungen des BSI erfüllt und entsprechend zertifiziert ist.

Entsprechende Listen von Anbietern sind verfügbar unter <http://www.ccepa.de/eid-service-anbieter>.

Abschließend noch ein Hinweis zu den Kosten. Im Moment sind verschiedene Zahlen im Umlauf. Für Kommunen, die Online-Services unter Nutzung der eID-Funktion anbieten wollen, werden zurzeit zwischen 6.000 und 8.000 Euro Kosten pro Jahr veranschlagt. Kenner der Szene gehen davon aus, dass diese Kosten deutlich verringert werden können - wenn die Nachfrage nach Zertifikaten und eID-Servern steigt.

## 9. Muster für eine Datenschutzerklärung

Die Kommune ABCDEFG, vertreten durch den (Ober-)Bürgermeister XYZ, nimmt den Schutz Ihrer personenbezogenen Daten sehr ernst. Wenn Sie [www.ABCDEFG.de](http://www.ABCDEFG.de) nutzen, verarbeitet die Stadt ABCDEFG Daten im Rahmen der gesetzlichen Bestimmungen. Maßgebliche Vorschriften dazu enthält das Telemediengesetz.

Im Folgenden wird erläutert, welche Daten während Ihres Besuches auf den Webseiten erfasst und verwendet werden.

### Datenerhebung und -verarbeitung bei Zugriffen aus dem Internet

Wenn Sie die Webseiten besuchen, speichern die Webserver temporär jeden Zugriff in einer Protokolldatei. Folgende Daten werden erfasst und bis zur automatisierten Löschung gespeichert:

- IP-Adresse des anfragenden Rechners
- Datum und Uhrzeit des Zugriffs
- Name und URL der abgerufenen Datei

Die Verarbeitung dieser Daten erfolgt zum Zweck, die Nutzung der Webseite zu ermöglichen (Verbindungsaufbau), der Systemsicherheit, der technischen Administration der Netzinfrastruktur sowie zur Optimierung des Internetangebotes. Die IP-Adresse wird nur bei Angriffen auf die Netzinfrastruktur der Kommune ABCDEFG ausgewertet.

Über die vorstehend genannten Fälle hinaus werden personenbezogene Daten nicht verarbeitet, es sei denn Sie willigen ausdrücklich in eine weitergehende Verarbeitung ein.

### Nutzung und Weitergabe personenbezogener Daten

Jegliche Nutzung Ihrer personenbezogenen Daten erfolgt nur zu den genannten Zwecken und in dem zur Erreichung dieser Zwecke erforderlichen Umfang.

Übermittlungen personenbezogener Daten an staatliche Einrichtungen und Behörden erfolgen nur im Rahmen zwingender nationaler Rechtsvorschriften oder wenn die Weitergabe im Fall von Angriffen auf unsere Netzinfrastruktur zur Rechts- oder Strafverfolgung erforderlich ist. Eine Weitergabe zu anderen Zwecken an Dritte findet nicht statt.

### Einwilligung in weitergehende Nutzung

Die Nutzung bestimmter Angebote auf [www.ABCDEFG.de](http://www.ABCDEFG.de) wie etwa Newsletter oder Foren erfordert eine vorherige Registrierung und weitergehende Verarbeitung personenbezogener Daten, beispielsweise eine längerfristige Speicherung von E-Mail-Adressen, Nutzerkennungen und Passwörtern. Die Verwendung solcher Daten erfolgt nur, wenn Sie der Kommune ABCDEFG diese übermittelt und vorab in die Verwendung eingewilligt haben.

### Newsletter und Presseverteiler

Um sich bei einem Newsletter-Dienst der Kommune ABCDEFG anzumelden, benötigen die Kommune ABCDEFG mindestens Ihre E-Mail-Adresse, an die der Newsletter versendet werden soll. Weitere Angaben sind freiwillig und werden verwendet, um sie persönlich anzusprechen und Rückfragen zur E-Mailadresse klären zu können. Bei postalischem Versand werden ihre Adressdaten benötigt. Bei Presseverteilern sind Angaben zum Presseorgan für das sie tätig sind erforderlich.

In der Regel verwendet die Kommune ABCDEFG für den Newsletter-Versand das Double Opt-In-Verfahren. D.h. Newsletter werden erst dann zugesandt, wenn Sie Ihre Anmeldung nach Mitteilung Ihrer E-Mail-Adresse über eine von der Kommune ABCDEFG zugesendete E-Mail und einen darin enthaltenen Link bestätigen. Damit soll sichergestellt werden, dass nur Sie selbst sich als Nutzer der angegebenen E-Mail-Adresse bei dem Newsletter-Dienst anmelden können. Ihre Bestätigung muss zeitnah zur Übersendung der E-Mail durch die Kommune ABCDEFG erfolgen, da andernfalls Ihre Anmeldung und E-Mail-Adresse in der Datenbank gelöscht wird. Bis zu einer Bestätigung durch Sie, nimmt der Newsletter-Dienst keine weiteren Anmeldungen unter dieser E-Mail-Adresse entgegen.

Sie können einen bei der Kommune ABCDEFG abonnierten Newsletter jederzeit abbestellen. Die Stornierung können Sie entweder per E-Mail oder über einen Link am Ende des Newsletters vornehmen.

### **Gästebücher und Foren**

Um sich für ein Internet-Forum der Kommune ABCDEFG zu registrieren, benötigen wir mindestens eine Nutzerkennung, ein Kennwort sowie Ihre E-Mail-Adresse. Die Registrierung zu einem solchen Dienst kann zu Ihrem Schutz entsprechend der Anmeldung bei einem Newsletter-Dienst nur erfolgen, wenn Sie Ihre Anmeldung über eine von der Kommune ABCDEFG zugesendete E-Mail und den darin enthaltenen Link bestätigen.

Sie können die genannten Dienste jederzeit kündigen, indem Sie eine E-Mail über die entsprechende Webseite des Dienstes zusenden.

Gästebücher und Foren unterliegen grundsätzlich keiner inhaltlichen Kontrolle der Kommune ABCDEFG. Gleichwohl behalten wir uns vor, nach eigenem Ermessen Einträge zu löschen und Nutzer von der weiteren Nutzung auszuschließen, insbesondere wenn Einträge strafrechtlich relevante Tatbestände erfüllen oder mit den Zielen der Kommune ABCDEFG nicht zu vereinbaren sind.

### **Bestellungen**

Die Kommune ABCDEFG erhebt bei der Online-Theaterkartenbestellung über Sie nur die personenbezogenen Daten, welche Sie selbst von sich aus in unsere Bestellformulare eingeben. Hierbei sind nur die Angaben, die zur Abwicklung des betreffenden Geschäfts zwingend erforderlich sind, als Pflichtangaben ausgestaltet. Alle möglicher Weise darüber hinaus gehenden Angaben können Sie auf rein freiwilliger Basis machen.

Mit der Eingabe Ihrer personenbezogenen Daten erklären Sie sich mit der Verarbeitung Ihrer personenbezogenen Daten entsprechend dieser Datenschutzerklärung der Kommune ABCDEFG einverstanden.

Wir übermitteln Ihre personenbezogenen Daten nur dann an unsere Dienstleistungs- und Partnerunternehmen, sofern dies zur Bestellungsabwicklung und zur Betreuung unserer Kunden bei der Vertragserfüllung zwingend erforderlich ist. Diese Unternehmen dürfen Ihre personenbezogenen Daten ausschließlich zu diesem Zweck nutzen und sind ebenfalls verpflichtet, alle anwendbaren Datenschutzbestimmungen einzuhalten.

Bei der Online-Theaterkartenbestellung erheben wir sämtliche personenbezogenen Daten zu Ihrer Sicherheit selbstverständlich unter Verwendung einer sicheren und verschlüsselten SSL-Verbindung (erkennbar am Beginn der Internetadresse mit „https://“ oben in der Adresszeile Ihres Internet-Browsers).



Sofern sie Informationsmaterialien bestellen, verwenden wir die dabei angegebenen Adressdaten nur zur Abwicklung der Bestellung. Eine Weitergabe an Dritte erfolgt nicht.

### **Sicherheit**

Die Kommune ABCDEFG setzt technische und organisatorische Sicherheitsmaßnahmen ein, um personenbezogenen Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Die Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

### **Cookies**

Auf [www.ABCDEFG.de](http://www.ABCDEFG.de) werden lediglich ausnahmsweise Session-Cookies eingesetzt, die Daten zur technischen Sitzungssteuerung im Speicher Ihres Browsers ablegen. Diese Daten sind nicht personenbezogen und werden spätestens mit dem Schließen Ihres Browsers gelöscht.

Sollten ausnahmsweise in einem Cookie auch personenbezogene Daten gespeichert werden, etwa eine Nutzerkennung, wird vorab ihre Einwilligung erfragt.

Sie können das Speichern von Cookies verhindern, indem Sie dies in Ihren Browser-Einstellungen festlegen. Wenn Sie keine Cookies akzeptieren, kann dies zu Funktionseinschränkungen des Angebotes führen.

### **Links zu Webseiten anderer Anbieter**

Dieses Internet-Angebot enthält Links zu Web-Angeboten, die außerhalb der Verantwortlichkeit der Kommune ABCDEFG bereitgestellt werden. Externe Seiten werden in einem eigenen Browserfenster geöffnet und sind an dem Symbol zu erkennen. Wir weisen darauf hin, dass diese Datenschutzerklärung ausschließlich für die Webseiten der Kommune ABCDEFG gilt.

Bei der erstmaligen Verknüpfung entsprechender Angebote, prüfen wir die fremden Inhalte daraufhin, ob durch sie eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Verweise fügen wir nur dann auf unseren Seiten ein, wenn zum Zeitpunkt der Verknüpfung keine Bedenken in der oben genannten Hinsicht bestehen.

Die verlinkten Angebote können sich jedoch dynamisch ändern. Eine Verpflichtung, auch diese Änderungen auf zivilrechtliche oder strafrechtliche Belange zu prüfen, besteht nicht. Falls Ihnen ein möglicher zivilrechtlicher oder strafrechtlicher Verstoß in den verlinkten Angeboten auffällt, wären wir für einen entsprechenden Hinweis dankbar.

### **Auskunftsrecht und Kontaktdaten**

Ihnen steht ein Auskunftsrecht bezüglich der über Sie gespeicherten personenbezogenen Daten, das Recht auf Berichtigung unrichtiger Daten, Sperrung und Löschung zu.

Wenn Sie Auskunft über Ihre personenbezogenen Daten beziehungsweise deren Korrektur oder Löschung wünschen oder weitergehende Fragen über die Verwendung Ihrer uns überlassenen personenbezogenen Daten haben, kontaktieren Sie bitte die behördliche Datenschutzbeauftragte

Hier einfügen: Angaben zum Datenschutzbeauftragten der Kommune ABCDEFG (Name, Anschrift, Telefon, Mailadresse)

Sollten Sie mit der Kommune ABCDEFG per E-Mail in Kontakt treten wollen, wird darauf hingewiesen, dass der Inhalt unverschlüsselter E-Mails von Dritten eingesehen werden kann. Es wird empfohlen, vertrauliche Informationen über den Postweg zuzusenden.

### **Gültigkeit und Aktualität der Datenschutzerklärung**

Mit der Nutzung unserer Webseite willigen Sie in die vorab beschriebene Datenverarbeitung ein. Die Datenschutzerklärung ist aktuell gültig und datiert vom XX.YY.1234.

Durch die Weiterentwicklung unserer Webseite oder die Implementierung neuer Technologien kann es notwendig werden, diese Datenschutzerklärung zu ändern. Die Kommune ABCDEFG behält sich vor, die Datenschutzerklärung jederzeit mit Wirkung für die Zukunft zu ändern. Wir empfehlen Ihnen, sich die aktuelle Datenschutzerklärung von Zeit zu Zeit erneut durchzulesen.

Bearbeitungsstand:  
April 2011

Ansprechpartnerin:  
Dipl.-Pol. Christine Siegfried, Vitako, siegfried@vitako.de

Vitako ist die Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister. Mehr als 50 Rechenzentren, Software- und Serviceunternehmen mit 7.000 Beschäftigten aus 14 Bundesländern bündeln in dem rechtsfähigen Verein ihr Know-how und stellen es den Kommunen zur Verfügung. Vitako berät und unterstützt die Kommunalen Spitzenverbände bei der Wahrnehmung ihrer Aufgaben in zahlreichen Fragen der Informations- und Kommunikationstechnik. Insgesamt betreuen die Mitgliedsunternehmen über 500.000 IT-Arbeitsplätze in mehr als 10.000 Kommunen und ein jährliches Umsatzvolumen von rund einer Milliarde Euro.