ID-Safe für SiXFORM

Prozessbeschreibung und Sicherheitskonzept

SiXFORM GmbH

Impressum

Herausgeber		
SiXFORM Technologiepark 1, D-91522 Ansbach		
Dateiname	**Dokumentennummer**	**Dokumentenbezeichnung**
20130415ID-Safe.docx	ID-Safe0002	ID-Safe für SiXFORM
Version	**Stand**	**Status**
1.1	15.04.2013	Abgestimmt
Autor	**Inhaltlich geprüft von**	**Freigegeben von**
Rudolf Philipeit	Rudolf Philipeit	Rudolf Philipeit
Ansbach	15.04.2013	15.04.2013
Ansprechpartner	**Telefon / Fax**	**E-Mail**
Rudolf Philipeit	Tel.: +49 (981) 4815500 Fax: +49 (981) 4815000	rudolf.philipeit@sixform.com
Kurzinfo		
Prozessbeschreibung und Sicherheitskonzept ID-Safe für SiXFORM		

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die in diesem Dokument beschriebene Lösung *ID-Safe für SiXFORM*[1] ermöglicht Kommunen zum Zwecke eines weitergehenden elektronischen Identitätsmanagements einen „ID Safe“ für ihre Bürgerinnen und Bürger bereitzustellen. Damit wird es für die Bürgerinnen und Bürger möglich mit Hilfe ihres neuen Personalausweises bei freigeschalteter eID-Funktion verifizierte Daten im Wege des elektronischen Identitätsnachweises in den ID-Safe einzustellen und diese für vielfältige elektronische Vorgänge im kommunalen Umfeld wieder zu verwenden. Der ID-Safe für SiXFORM ist hierbei in der Art und Weise ausgebildet, dass die Zurverfügungstellung der Daten durch die Ausweisinhaber für jeden elektronischen Vorgang auf deren bewusster, informierter Basis erfolgt. D. h. der Ausweisinhaber selbst muss für jeden Vorgang aktiv eine eigene Freigabe seiner Daten erteilen (Zäsur zwischen elektronischem Identitätsnachweis und benutzerkontrollierter Weiterverwendung/informationeller Selbstbestimmung)

2 Berechtigungszertifikat zum Auslesen des nPA / Geschäftszweck

Um als Diensteanbieter (z.B. Stadt, Landkreis usw.) die Daten aus einem neuen Personalausweis auslesen zu dürfen ist ein Berechtigungszertifikat erforderlich. Das Berechtigungszertifikat muss vom Diensteanbieter beim Bundesverwaltungsamt beantragt werden. Hierfür muss ein klar darstellbarer Geschäftszweck vorgetragen werden. Für den ID-Safe für SiXFORM wird der Geschäftszweck aus der VITAKO[2]-Veröffentlichung "Beantragung von Zertifikaten für das Auslesen von Daten aus dem neuen Personalausweis" (Stand April 2011) uneingeschränkt verwendet:

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.

Für den ID-Safe für SiXFORM lautet der Geschäftszweck:

Anlegen und Nutzung eines ID-Safes zur Abwicklung von Online-Services

Die SiXFORM GmbH kann für die Diensteanbieter, welche den ID-Safe für SiXFORM einsetzen wollen, die vollständige Antragstellung im Auftrag durchführen.

[1] SiXFORM (Signierbare XML-Formulare) ist ein Lösungsansatz um mit standardisierten Datencontainern (PDF 1.7, ISO 32000) medienbruchfreie Prozessketten herzustellen.
[2] VITAKO: Bundesarbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

3 Prozessbeschreibung

Die Nutzung des ID-Safe für SiXFORM sieht folgende Abläufe vor:

3.1 Nutzung einer Verwaltungsleistungen über den ID-Safe unter Nutzung des neuen Personalausweises

Der Antragsteller kann eine Verwaltungsleistung/Dienstleistung mit Unterstützung seines ID-Safes abwickeln. Der ID-Safe bietet die Möglichkeit sehr komfortabel qualitätsgesicherte und vertrauenswürdige Daten für Vorgänge mit seiner Behörde zur Verfügung zu stellen. Nach Auswahl einer Verwaltungsleistung erhält der Nutzer die beiden Auswahlmöglichkeiten

- *Neuregistrierung* (*erstmaliger Besucher)* und
- *Nutzung der bereits hinterlegten Daten* (*wiederkehrender Besucher)*

angezeigt. Entsprechend der Auswahl verzweigt der weitere Ablauf in einen der beiden nachfolgend beschriebenen Teilprozesse. Wurde eine nicht zutreffende Auswahl getroffen, wird nach dem Einlesen der Daten aus dem Personalausweis der Fehler durch das Programm erkannt und der Nutzer wird auf den Fehler hingewiesen. Danach muss von vorne mit dem Vorgang begonnen werden.

3.1.1 Neuregistrierung (erstmaliger Besucher)

Für die Neuregistrierung werden dem Bürger zunächst die Informationen zum Datenschutz und die Nutzungsbedingungen angezeigt. Der erstmalige Benutzer wird auch darüber informiert, dass der ID-Safe für die Vorgänge mit der Behörde vertrauenswürdige Daten ermöglicht. Damit wird in vielen Fällen bereits eine Antragstellung ohne handschriftliche Unterschrift möglich und erspart somit für den Antragsteller Wege zum Amt und den damit verbundenen Zeitaufwand. Zusätzlich wird der Antragsteller darüber informiert, dass seine Daten für zukünftige Vorgänge im ID-Safe sicher gespeichert werden und über einen extra Zugang mit weiteren Daten, wie z.B. Telefonnummern und die bevorzugte Erreichbarkeit, ergänzt werden können. Sobald die Kenntnisnahme und Akzeptanz der Informationen vom Ausweisinhaber bestätigt wurden, werden die Daten aus dem nPA in den ID-Safe übernommen. Der Ausweisinhaber wird hierüber informiert und um Bekanntgabe seiner E-Mail-Adresse gebeten. Zur Bestätigung der korrekten E-Mail-Adresse wird eine Nachricht mit einem zu bestätigenden Link an die E-Mail-Adresse gesandt (Double-Opt-In-Verfahren). Sobald über den Link die E-Mail-Adresse bestätigt wurde, wird der ID-Safe aktiv geschaltet.

3.1.2 Nutzung der bereits hinterlegten Daten (wiederkehrender Besucher)

Die im ID-Safe gespeicherten Daten stehen für die Nutzung der formular-basierenden Vorgänge zwischen Bürgerinnen und Bürger mit der Verwaltung zur Verfügung. Für die Zurverfügungstellung der Daten ist das DKK des nPA ausreichend. Bevor die Daten zum Einsatz kommen wird der jeweilige Antragsteller auf die Verwendung seiner Daten für den jeweiligen Vorgang um eine Datenfreigabe gebeten.

3.2 Datenpflege der Daten im ID-Safe unter Nutzung des neuen Personalausweises

Der Zugang zur Datenpflege erfolgt über den neuen Personalausweis. Das dienste- und kartenspezifische Kennzeichen ist für den Zugang ausreichend. Wurde ein neuer Personalausweis ersetzt, so werden wieder alle Daten zur Identifikation einer Person für die "Bekanntmachung" des Nachfolgeausweises benötigt.

4 Prozessdarstellung

Die Nutzung des ID-Safe für SiXFORM sieht folgende Nutzungsvarianten vor:

Abbildung 1: Darstellung der Nutzungsvarianten

5 Sicherheitskonzept

5.1 IT-Richtlinie

5.1.1 Einleitung

Diese IT-Richtlinie soll die von der SiXFORM GmbH getroffenen Maßnahmen zum Schutz von (personenbezogenen) Daten im ID-Safe vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeiter unterstützen und darüber hinaus eine grundlegende Information für unsere Kunden im Hinblick auf den Umgang mit Daten im ID-Safe sein.

5.1.2 Geltungsbereich

Diese IT-Richtlinie gilt für alle Beschäftigte der SiXFORM GmbH. Dazu gehören alle Festangestellte, Teilzeitangestellte, Auszubildende, Werkstudenten sowie Aushilfskräfte etc. Auch externe Personen, die regelmäßig in unserem Unternehmen tätig sind, sind verpflichtet, sich an diese Richtlinie zu halten. Die SiXFORM GmbH wird entsprechende Vorkehrungen treffen, damit diese Richtlinie auch für die externen Personen verbindlichen Charakter hat.

5.1.3 Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen der SiXFORM GmbH sind von den Mitarbeitern die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Sollten Mitarbeiter unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Vorgesetzten zur Klärung zu wenden.

5.1.4 Schulung

Das Unternehmen trägt Sorge dafür, dass die Mitarbeiter die erforderlichen Schulungen und Instruktionen/Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind.

5.1.5 Allgemeine Regelungen

Die Nutzung der IT-Systeme und Applikationen der SiXFORM GmbH ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der ausdrücklichen Erlaubnis des Arbeitgebers, die schriftlich erfolgen muss.

Die Installation von Software zu privaten Zwecken ist untersagt. Im Übrigen darf nur die Software auf IT-Systemen der SiXFORM GmbH installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist.

Die Benutzung privater Hard-und Software zu dienstlichen Zwecken ohne Genehmigung des Arbeitgebers ist nicht zulässig.

5.1.6 Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern der SiXFORM GmbH so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem

Verlassen des Arbeitsplatzes grundsätzlich zu verschließen. Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter sich „abmelden“, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme – so auszurichten, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte nach Möglichkeit ausgeschlossen wird.

Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

5.1.7 Passwort-Gebrauch

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Die IT-Abteilung wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.

Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, das sie nicht durch Dritte leicht zu erraten sind. Vor-und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Passwörter sollten regelmäßig gewechselt werden. Bereits genutzte Passwörter dürfen nicht noch einmal wieder verwendet werden.

5.1.8 Schutz vor Schad-Inhalten

Zum Schutz vor Schad-Inhalten werden in der SiXFORM GmbH Virenschutz-programme eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutzprogramme überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen. Für den Fall, dass ein Mitarbeiter eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang erhält, ist dieser verpflichtet, sich unverzüglich an die IT-Abteilung zu wenden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Freigabe durch die IT-Abteilung geöffnet werden.

5.1.9 Schutz vor unverlangter Werbung („Spam“)

Zum Schutz vor unverlangter Werbung durch E-Mail werden im Unternehmen so genannte Spam-Filter eingesetzt. Der Einsatz des Spam-Filters erfolgt aus betrieblichen Gründen. Durch den Spam-Filter kann es dazu kommen, dass im

Einzelfall E-Mails unterdrückt oder gelöscht werden. Die Mitarbeiter sollen Sorge dafür tragen, dass zum Beispiel beim erwünschten Erhalt von E-Mail-Newsletter die entsprechenden Absender-Adressen in ihr E-Mail-Adressbuch gespeichert werden, um fehlerhafte Klassifizierungen zu vermeiden.

5.1.10 Nutzung von E-Mail/Internet

Soweit nicht ausdrücklich eine Zustimmung des Unternehmens erfolgt ist, darf die Nutzung von E-Mail und Internet nur für dienstliche Zwecke erfolgen.

Den Mitarbeitern wird gestattet, private E-Mails über ihren eigenen, privaten Webmail-Account zu empfangen und zu senden. Der Umfang dieser Nutzung ist aus betrieblichen Gründen von der SiXFORM GmbH auf die Pausenzeiten beschränkt worden.

5.1.11 Verhalten bei Sicherheitsvorfällen

Sollte der Mitarbeiter merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an die IT-Abteilung und seinen Vorgesetzten zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

5.1.12 Weisungen

Die Mitarbeiter sind verpflichtet, den Weisungen der IT-Abteilung Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen der IT-Abteilung bestehen, kann der Leiter der IT-Abteilung eingebunden werden.

5.2 Technische und organisatorische Maßnahmen

Der ID-Safe wird in einem Hochleistungs-Rechenzentrum der Deutschen Telekom/T-Systems in Magdeburg, Lübecker Straße 2, betrieben. Die technischen und organisatorischen Maßnahmen werden fast ausschließlich durch das Rechenzentrum vorgegeben.

5.2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Umsetzung im Rechenzentrum:

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Schließsystem mit Codesperre
- Manuelles Schließsystem
- Biometrische Zugangssperren
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen

5.2.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Umsetzung im Rechenzentrum:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal

- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrustion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Umsetzung durch die Anwendung ID-Safe:

- Authentifikation der Benutzer nur über das Dienste- und Kartenspezifische Kennzeichen des neuen Personalausweises möglich
- Einsatz von VPN-Technologie

5.2.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umsetzung im Rechenzentrum:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

Umsetzung durch die Anwendung ID-Safe:

- Authentifikation der Benutzer nur über das Dienste- und Kartenspezifische Kennzeichen des neuen Personalausweises möglich.
- Jeder Nutzer kann nur seine Daten mit Hilfe der Onlinefunktion seines neuen Personalausweises entschlüsseln und damit für einen Vorgang nutzbar machen.
- Administratoren haben keinen „Schlüssel“ und damit keinen Zugriff auf die personenbezogenen Daten der Nutzer des ID-Safes

5.2.4 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert,

verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Umsetzung im Rechenzentrum:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- E-Mail-Verschlüsselung
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

Umsetzung durch die Anwendung ID-Safe:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln

5.2.5 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umsetzung im Rechenzentrum:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Umsetzung durch die Anwendung ID-Safe:

- Diesbezügliche Daten werden bewusst nicht gespeichert (damit soll auf Dauer ein hohes Vertrauen bei den Nutzern hergestellt werden). Sollte ein Missbrauch entstehen wird die Auswirkung in den dem ID-Safe nachgelagerten Nutzungsmomenten der Daten erkannt und ausgeregelt.

5.2.6 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Umsetzung im Rechenzentrum:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertragsstrafen bei Verstößen

5.2.7 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Umsetzung im Rechenzentrum:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze

5.2.8 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umsetzung im Rechenzentrum:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Umsetzung durch die Anwendung ID-Safe:

- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung aller Datensätze. Das Dienste- und Kartenspezifische Kennzeichen aus dem neuen Personalausweis wird hierbei als Schlüssel verwendet. Somit ist es nur dem Eigentümer des Ausweises und nur während der Verbindung (Session) möglich, die Daten aus dem ID-Safe zu entschlüsseln und für einen Vorgang zu verwenden.
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

6 Anhang

6.1 Muster für eine Datenschutzerklärung (Auszug einer Veröffentlichung von VITAKO im April 2011)

Die Kommune ABDCDEFG, vertreten durch den (Ober-)Bürgermeister XYZ, nimmt den Schutz Ihrer personenbezogenen Daten sehr ernst. Wenn Sie 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 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 ansprechen 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 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.

6.2 Auszug aus dem Telemediengesetz

§ 13 Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

(2) Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

(3) Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. Absatz 1 Satz 3 gilt entsprechend.

(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,

5. Daten nach § 15 Abs. 2 nur für Abrechnungszwecke zusammengeführt werden können und

6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.
(5) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.
(6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.
(7) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.
Nichtamtliches Inhaltsverzeichnis

Abkürzungsverzeichnis

HW	Hardware
ICT	Information and Communication Technologies
MoU	Memory of Understanding
PDF	Portable Document Format
SiXFORM	Signable XML Forms (signierbare XML-Formulare)
SW	Software
WSDL	Web Services Description Language
XML	Extensible Markup Language