STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

SächsEGovG

Handlungsleitfaden
zur Umsetzung in kommunalen Behörden

Version 1.0

Stand: 06. Februar 2015

Inhalt

Vorwort zum Handlungsleitfaden

Mit dem Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (SächsEGovG) vom 9. Juli 2014 (Seite 398 des SächsGVBl.) hat Sachsen als erstes Bundesland nach dem Bund, den rechtlichen Rahmen für den Einsatz elektronischer Verfahren in der sächsischen Verwaltung geschaffen.

Mit der E-Government-Gesetzgebung wurde nicht nur ein neues Rechtsgebiet geschaffen. Es wurde auch ein ambitioniertes Aufgabentableau beschlossen, das auf nahezu allen Verwaltungsebenen im Freistaat Sachsen einen merklichen Veränderungsprozess ausgelöst hat und weiter auslösen wird. Ziel dieses Prozesses ist die breite Fortentwicklung der Digitalisierung der öffentlichen Verwaltung im Freistaat Sachsen. Sie bezieht sich also nicht nur auf eine Verwaltungsfachebene, z. B. die Steuerverwaltung oder das Meldewesen. Sie betrifft vielmehr alle Verwaltungszweige – ganz gleich welchen Fachgebietes. Diese Fortentwicklung der Digitalisierung durch die öffentliche Verwaltung ist Kennzeichen des modernen Regierungs- und Verwaltungshandelns. Sie ist wesentlicher Standortfaktor für eine gute wirtschaftliche Entwicklung und eine lebenswerte Zukunft der Bürger im Freistaat Sachsen. Die Chancen, die die Digitalisierung den Bürgern und der Verwaltung bietet, wollen wir so noch besser nutzen.

Das Sächsische E-Government-Gesetz verpflichtet die Behörden und sonstigen öffentlichen Stellen im Freistaat Sachsen in unterschiedlicher Weise zur Umsetzung der neuen gesetzlichen Regelungen. Anspruch ist es, die Chancen von E-Government im Freistaat Sachsen bestmöglich nutzbar zu machen und ganzheitliche Potentiale für effektives und effizientes Verwaltungshandeln zu erschließen.

Der hier vorgelegte Handlungsleitfaden in der Version 1.0 beschreibt ausführlich diese Umsetzungspflichten für die kommunalen Behörden und gibt praktische Empfehlungen zu möglichen Umsetzungen aus Sicht des Freistaates Sachsen. Er geht dabei nicht auf die Anforderungen des E-Government-Gesetzes des Bundes ein, das nach seinem § 1 Abs. 2 auch für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts gilt, wenn sie Bundesrecht ausführen. Nicht behandelt werden zudem speziellere Vorschriften in Fachgesetzen oder z. B. nach §§ 71a ff. VwVfG, die ebenfalls die elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit der kommunalen Behörden regeln oder regeln können. Dies würde den Rahmen des auf die Umsetzung des Landesrechts beschränkten Handlungsleitfadens sprengen. Daher sei an dieser Stelle ergänzend z. B. auf die Ausführungen des BMI im sogenannten »Mini-Kommentar« zum E-Government-Gesetz des Bundes und die einschlägigen Fachkommentierungen verwiesen.

Es besteht zudem weder der Anspruch, jede Einzelfrage einer betroffenen Behörde zu beantworten noch alle behördenspezifischen Besonderheiten zu berücksichtigen, da sich die Vielfalt, der im Einsatz befindlichen und zudem heterogenen Technik, einer solchen Herangehensweise verschließt.

Der Handlungsleitfaden in seiner aktuellen Fassung wurde – aufbauend auf einer Vorgängerversion 0.5 – durch das Sächsische Staatsministerium des Innern (SMI) fertiggestellt. Ausgangspunkt für die Erarbeitung war eine Bitte des Sächsischen IT-Kooperationsrates. Zusammen mit der Sächsischen Anstalt für Kommunale Datenverarbeitung, den kommunalen Landesverbänden und unter Beteiligung des Sächsischen Datenschutzbeauftragten wurde er in thematischen Arbeitsgruppen erstellt. Die Federführung lag bei der Abteilung 6 (Informationstechnologie und E-Government in der Staatsverwaltung) des SMI.

Der Handlungsleitfaden behandelt insbesondere solche Regelungen,

- die für alle Träger der öffentlichen Verwaltung gelten,
- die Pflichtaufgaben sind und
- die sofort nach Verkündung des Gesetzes in Kraft treten.

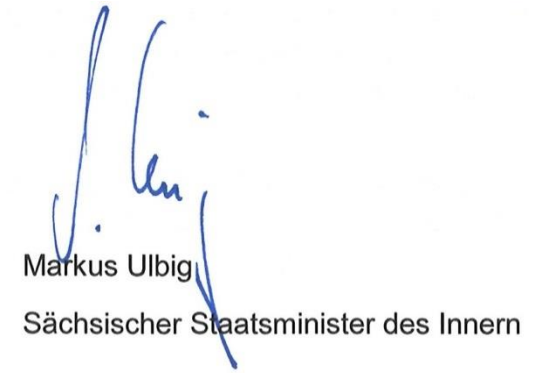
Der Handlungsleitfaden wird – ausgerichtet an den Bedürfnissen der Zielgruppen – schrittweise durch weitere Erläuterungen und Bausteine ergänzt. Eine nochmals erweiterte Folgeversion ist für das Jahr 2016 geplant, in dem weitere Regelungen des Gesetzes in Kraft treten.

Vorangestellt ist eine Übersicht zu den Umsetzungspflichten und -optionen des SächsEGovG für die kommunalen Behörden. Die Gliederung des Handlungsleitfadens erfolgt abschnittsweise nach den Paragraphen des SächsEGovG. Innerhalb dieser Abschnitte finden sich ein Erläuterungsteil zur jeweiligen Verpflichtung aus dem SächsEGovG, inhaltliche Ausführungen und Empfehlungen zur Umsetzung sowie Antworten auf allgemein interessierende Fragestellungen zum jeweiligen Thema (FAQ).

Das Dokument enthält auch Verweise auf Anlagen im Anhang des Handlungsleitfadens sowie auf weitere externe Dokumente und Webseiten. Diese Verweise sind als Hyperlink farblich und unterstrichen gekennzeichnet. Das Dokument ist barrierefrei und für jedermann frei zugänglich. Änderungen dürfen aber nicht vorgenommen werden und bei Vervielfältigung oder öffentlicher Wiedergabe ist § 5 Abs. 2 UrhG (Quellenangabe) zu beachten.

Ich bin zuversichtlich, dass der Handlungsleitfaden den Trägern der Selbstverwaltung im Freistaat Sachsen eine gute und wichtige Hilfestellung gibt, um die abstrakten Vorschriften des Sächsischen E-Government-Gesetzes in der täglichen Verwaltungspraxis mit Leben zu erfüllen. Bürger und Unternehmen müssen ihre Anliegen auch sicher über die elektronischen Kommunikationswege mit der Verwaltung abwickeln können. Der Handlungsleitfaden gibt hier die notwendige Orientierung.

In diesem Sinne hoffe ich auf eine gute Aufnahme des Handlungsleitfadens bei allen Akteuren, die sich dem Ziel eines guten Regierungs- und Verwaltungshandelns verpflichtet sehen.



Markus Ulbig

Sächsischer Staatsminister des Innern

Umsetzungspflichten und –optionen des SächsEGovG mit entsprechenden Fristen für kommunale Behörden

9. August 2014

Pflichten (»muss«)

- § 2 Absatz 1 – Elektronische Kommunikation grundsätzlich mit Verschlüsselung ermöglichen
- § 3 – Elektronische Zahlungen ermöglichen
- § 5 Absatz 1 – Datenschutz- und Informationssicherheitskonzepte erstellen
- § 7 – Elektronische Kommunikation und Dokumente barrierefrei gestalten
- §§ 9 Absatz 2, 13 Absatz 1 – Informationssicherheit gewährleisten
- § 15 – Anschluss an das Kommunale Datennetz oder über eine Schnittstelle an das Sächsische Verwaltungsnetz herstellen
- § 19 Absatz 3 – Voraussetzungen für die Verwendung der sorbischen Sprache schaffen

Optionen (»kann«)

- § 4 – Elektronische Publikationen anbieten
- § 6 – Gemeinsame Verfahren durchführen, dabei Datenschutz gewährleisten
- § 14 Absatz 1 – Basiskomponenten nutzen
- § 16 – Elektronische Vorgangsbearbeitung und Aktenführung einsetzen
- § 20 – Experimentierklausel nutzen

1. August 2016

Pflichten (»muss«)

- § 2 Absatz 2 – Elektronische Kommunikation mit Schriftformersatz ermöglichen (unter Haushaltsvorbehalt)

Empfehlungen zur Umsetzung des SächsEGovG für kommunale Behörden des Freistaates Sachsen

§ 1 SächsEGovG – Anwendungsbereich

§ 1 SächsEGovG lautet:

»(1) Dieses Gesetz regelt die elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Freistaates Sachsen sowie der seiner Aufsicht unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (Träger der Selbstverwaltung). Auf Beliehene finden die Vorschriften dieses Gesetzes für die Träger der Selbstverwaltung Anwendung.

(2) Dieses Gesetz gilt nicht für die Tätigkeit des Mitteldeutschen Rundfunks.

(3) Für die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung einschließlich der ihrer Aufsicht unterliegenden Körperschaften des öffentlichen Rechts gilt dieses Gesetz nur, soweit die Tätigkeit der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder durch die in verwaltungsrechtlichen Anwalts-, Patentanwalts- und Notarsachen zuständigen Gerichte unterliegt.«

A Erläuterung der Verpflichtung

Regelungsgegenstand des Gesetzes

§ 1 SächsEGovG bestimmt den Regelungsgegenstand und die Adressaten des Gesetzes.

Das Gesetz regelt die elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit, die sächsische Behörden und sonstige öffentliche Stellen nach Maßgabe des SächsEGovG ausüben müssen oder sollen. Es enthält zudem auch Regelungen zur Erfüllung der Aufgaben in Ausübung pflichtgemäßen Ermessens.

E-Government – nach § 1 Abs. 1 SächsEGovG verstanden als die »elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit« – soll nach Maßgabe der Regelungen in den §§ 2 ff. SächsEGovG im Freistaat Sachsen gefördert und befördert werden.

Adressat des Gesetzes

Adressat und damit Verpflichteter des Gesetzes sind die Behörden des Freistaates Sachsen sowie die seiner Aufsicht unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (Träger der Selbstverwaltung). Der in § 1 Abs. 1 S. 1 SächsEGovG bestimmte Anwendungsbereich geht von der wortgleichen Formulierung in § 1 S. 1 SächsVwVfZG aus und orientiert sich begrifflich an den verfassungsrechtlichen Vorgaben für die sächsische Verwaltung.

Demnach wird die Verwaltung im Freistaat Sachsen gemäß Art. 82 Abs. 1 S. 1 SächsVerf durch die staatlichen Behörden und die Träger der Selbstverwaltung ausgeübt. Träger der Selbstverwaltung sind gemäß Art. 82 Abs. 2 S. 1 SächsVerf die Gemeinden, Landkreise und andere Gemeindeverbände (als kommunale Träger der Selbstverwaltung) und nach Art. 82 Abs. 3 SächsVerf andere öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen (nach Maßgabe der Gesetze als nichtkommunale Träger der Selbstverwaltung).

Damit ist ausschließlich die »sächsische öffentliche Hand«, d. h. alle sächsischen Behörden und Verwaltungseinrichtungen der unmittelbaren und mittelbaren Verwaltung im Freistaat Sachsen Adressat des Gesetzes (z. B. auch Landtagsverwaltung, Rechnungshof, kommunale Eigenbetriebe, Kammern).

a) Ausnahme MDR

Nach § 1 SächsEGovG gilt das Gesetz nicht für den Mitteldeutschen Rundfunk (MDR).

b) Spezialfall Beliehener

Das Gesetz gilt für Private nur insofern, als dass sie Beliehene sind. Beliehene, d. h. natürliche oder juristische Personen des Privatrechts, denen durch oder aufgrund eines Gesetzes hoheitliche Befugnisse übertragen wurden, werden vom Anwendungsbereich des Gesetzes umfasst. Je nach beleihendem Verwaltungsträger sind sie entweder dem Freistaat Sachsen selbst zuzurechnen oder den Trägern der Selbstverwaltung. Das Gesetz regelt, dass auf alle Beliehenen nach § 1 Abs. 1 S. 2 SächsEGovG ausschließlich die Vorschriften für die Träger der Selbstverwaltung Anwendung finden. In diesen Vorschriften sind weniger strenge Verpflichtungen enthalten als für die Staatsbehörden; sie eröffnen den Beliehenen daher größere Spielräume. Die Beliehenen müssen mithin unabhängig von dem sie beleihenden Rechtsträger neben den allgemeinen Vorschriften, insbesondere des Abschnittes 1 des SächsEGovG (Allgemeine Regelungen) nur die Vorgaben des Abschnittes 3 (Regelungen für die Träger der Selbstverwaltung) beachten und umsetzen.

c) Besonderheiten der Justiz

Durch § 1 Abs. 3 SächsEGovG wird die Tätigkeit der Justiz teilweise vom Anwendungsbereich dieses Gesetzes ausgenommen. Die Regelung entspricht dem wortgleichen § 2 Abs. 3 Nr. 1 VwVfG und gewährleistet den Schutz der Judikative, die wie die Legislative eigenständig neben der von diesem Gesetz erfassten Exekutive steht. Gleichzeitig sichert die Formulierung ab, dass dieses Gesetz genauso wie das Verwaltungsverfahrensgesetz für den zur Exekutive zählenden Bereich der Justizverwaltung gilt. Aus § 1 Abs. 3 SächsEGovG ergibt sich also, dass dieses Gesetz für die Tätigkeit der Gerichtsverwaltungen und für die Behörden der Justizverwaltung gilt, wenn und soweit die jeweilige Tätigkeit der Nachprüfung durch die im Gesetzestext erwähnten Gerichte unterliegt.

Geltungsbereich des Gesetzes

a) Verhältnis zu anderen Vorschriften

In § 19 SächsEGovG selbst wird das Verhältnis der Vorschriften des SächsEGovG zu den schon bisher im Freistaat Sachsen geltenden, allgemein verfahrensrechtlichen Gesetzesvorschriften im E-Government-Bereich geregelt. Bei §§ 19 Abs. 1 und 2 SächsEGovG handelt es sich um deklaratorische Verweisungen, die lediglich darauf hinweisen, dass weitere Gesetzestexte zu beachten sind. So verdeutlicht § 19 Abs. 1 SächsEGovG, dass das SächsEGovG den Regelungsgehalt des § 3a VwVfG (Elektronische Kommunikation), der aufgrund der dynamischen Verweisung in § 1 S. 1 SächsVwVfZG auch im Freistaat Sachsen gilt, nicht ändert, sondern lediglich ergänzt (siehe Abschnitt A zu § 2 Abs. 2 SächsEGovG).

§ 19 Abs. 2 SächsEGovG regelt das Verhältnis des Gesetzes zu § 123 Abs. 5 SächsGemO. Die in § 123 Abs. 5 SächsGemO vorgesehene Möglichkeit der Aufsichtsbehörden, den Gemeinden Maßgaben zur elektronischen Datenverarbeitung vorzugeben, wird durch die Regelungen des SächsEGovG nicht berührt. Die dort eröffneten Befugnisse gelten weiterhin vollumfänglich. Dies gilt auch für entsprechende Vorgaben der Aufsichtsbehörden an die Landkreise über § 65 Abs. 2 S. 1 SächsLKrO i. V. m. § 123 Abs. 5 SächsGemO.

b) Vorrang des Fachrechts

Im SächsEGovG ist – anders als im Bundesrecht (vgl. § 1 Abs. 4 EGovG) – keine Kollisionsvorschrift enthalten, die das Anwendungsverhältnis des SächsEGovG zum Fachrecht regelt, das ebenfalls Vorschriften für die elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit enthält (Ausnahme: § 8 Abs. 4 SächsEGovG). Sofern es sich um Landesrecht verdrängende bundes- oder europarechtliche E-Government-Regelungen handelt, gehen diese dem SächsEGovG vor. Handelt es sich aber um gleichrangige Vorschriften des Landesrechts, die jeweils unterschiedliche Rechtsfolgen anordnen, muss entschieden werden, welchem Gesetz der Anwendungsvorgang zukommt. Sofern das Fachgesetz die Rechtsmaterie abschließend regelt, geht dieses dem SächsEGovG auch dann vor, wenn es vor Inkrafttreten des SächsEGovG erlassen wurde. Sofern das Fachgesetz die Rechtsmaterie jedoch nicht abschließend regelt, gilt über die Regeln des Fachrechts hinaus (zusätzlich) das SächsEGovG. Ob eine Norm abschließenden Charakter hat, ist durch Auslegung zu ermitteln.

B Empfehlungen zur Umsetzung

Konkrete Adressaten in der jeweiligen Behörde

In erster Linie richtet sich das Gesetz an die Amts- und Behördenleiter, Bürgermeister, Landräte und Verbandsvorsitzenden, die anhand einer Prüfung der einzelnen Vorschriften für ihre Behörde oder öffentliche Stelle klären müssen, welche Verpflichtungen und welche Möglichkeiten sie aus den Paragraphen des Gesetzes haben, um E-Government zu befördern.

Dabei ist zu berücksichtigen, dass nicht alle Regelungen gleichermaßen für alle Adressaten gelten und nicht alle Normen Pflichten regeln:

a) So trifft beispielsweise alle staatlichen und kommunalen Verwaltungseinrichtungen die Verpflichtung, ab dem 9. August 2014 die elektronische Kommunikation mit Bürgern barrierefrei zu ermöglichen (§ 2 Abs. 1 i. V. m. § 7 SächsEGovG).

b) Kommunen und Landkreise sind nicht verpflichtet, sondern können von der Möglichkeit Gebrauch machen, ihre nach Maßgabe einzelner Rechtsvorschriften bestimmte Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt zusätzlich oder sogar ausschließlich auch dadurch zu erfüllen, indem sie eine elektronische Ausgabe des »amtlichen Bekanntmachungsblattes« führen (vgl. im Einzelnen § 4 SächsEGovG).

c) Soweit sich die Kommunen, Landkreise, Gemeindeverbände oder sonstige Träger der Selbstverwaltung (z. B. Hochschulen, Kammern) beispielsweise dafür entscheiden, die elektronische Vorgangsbearbeitung und Aktenführung einzuführen, sind sie an die für die Staatsbehörden entsprechend geltenden Vorschriften gebunden (§ 16 i. V. m. § 12 Abs. 1 S. 2, Abs. 4 und 5 SächsEGovG).

d) Die Experimentierklausel in § 20 SächsEGovG richtet sich dagegen nur an die Ressorts der Staatsverwaltung und den Beauftragten für Informationstechnologie. Denn nur auf oberster Staatsebene kann durch Rechtsverordnung entschieden werden, ob und wie von Kosten-, Zuständigkeits-, Form- und sonstigen landesrechtlichen Verfahrensvorschriften auch in Fachgesetzen befristet, sachlich und räumlich begrenzt abgewichen werden kann, um E-Government-Anwendungen einzuführen oder weiterzuentwickeln.

C Beantwortung häufig gestellter Fragen

Frage 1: Richtet sich die Verschlüsselung bei der Übermittlung von Passbildern zwischen Pass- und Ordnungsbehörde in Bußgeldverfahren nach dem Sächsischen E-Government-Gesetz oder nach dem Passgesetz des Bundes und welches Verschlüsselungsniveau gilt hier?

> **Antwort**: Die Pflicht zur Verschlüsselung bei der Übermittlung von Passbildern der Passbehörde an die Ordnungsbehörde richtet sich nicht nach § 2 Abs. 1 S. 2 SächsEGovG, sondern nach den bundesrechtlichen Vorschriften der §§ 22 Abs. 2, 22a Abs. 1 S. 2, 6a Abs. 1 S. 3 PassG, da nach Art. 31 GG Bundesrecht entgegenstehendes Landesrecht bricht und gleichlautendes zumindest verdrängt. Hier wie dort existiert jedoch keine Regelung, welches Verschlüsselungsniveau gilt (niedrig, mittel oder hoch). Dies gilt auch für den Fall, dass die Datenübermittlung nicht über das Internet, sondern über verwaltungsinterne Netze erfolgt (Siehe FAQ Nr. 1 und 2 zu § 2 Abs. 1 SächsEGovG, deren Antwort auch im Fall der Datenübermittlung über das Verwaltungsnetz einen bestimmten Grad der Verschlüsselung empfiehlt, aber rechtlich – von Maßnahmen der Fachaufsicht abgesehen – nicht vorschreiben kann).

Frage 2: Sowohl § 7 SächsEGovG als auch § 7 SächsIntegrG enthalten Regeln über die Barrierefreiheit. Verdrängt das SächsEGovG als das zeitlich später erlassene Gesetz das SächsIntegrG?

> **Antwort**: Nein. Beide Gesetze gelten nebeneinander, da die Rechtsfolgen die gleichen sind. Die bereits in § 7 SächsIntegrG verankerte Verpflichtung zur Barrierefreiheit ist derzeit bei einem elektronischen Zugang als Teil des Internetauftritts der Behörde verpflichtend. Darüber hinaus gilt § 7 SächsIntegrG aber dann nicht, wenn eine Behörde einen Zugang über eine andere elektronische Möglichkeit – unabhängig vom Internet – wählt, beispielsweise bei Bezahlmöglichkeiten, Akteneinsicht oder Verwaltungspostfächern. Daher wird durch §§ 1 Abs. 1, 7 SächsEGovG nunmehr eine barrierefreie Zugangseröffnung über die Regelung des § 7 SächsIntegrG hinaus gewährleistet (inhaltliche Erweiterung). Zudem soll die elektronische Kommunikation nicht nur den Staatsbehörden, sondern insbesondere auch der kommunalen Verwaltung mit dem behinderten Bürger barrierefrei ermöglicht werden (Erweiterung des Adressatenkreises).

Frage 3: Unter den Voraussetzungen des § 4 SächsEGovG ist es beispielsweise möglich, kommunale Satzungen einer Gemeinde auch oder sogar ausschließlich elektronisch zu verkünden. Widerspricht dies nicht § 2 der Kommunalbekanntmachungsverordnung (KomBekVO), die für öffentliche Bekanntmachungen von Satzungen nur den Abdruck (also eine Papierfassung), z. B. im Amtsblatt der Gemeinde oder des Landkreises, dem die Gemeinde angehört, vorschreibt?

> **Antwort**: In gewisser Weise ja. Aber die KomBekVO hatte bei ihrem Erlass im Jahre 1997 elektronische Bekanntmachungen nicht im Blick.
> Die KomBekVO geht als Rechtsverordnung der gesetzlichen Regelung des SächsEGovG nach. Da § 4 SächsEGovG zeitlich später als die auf § 127 Abs. 1 Nr. 3 SächsGemO zu stützende KomBekVO erlassen wurde, der Gesetzgeber beim Erlass des SächsEGovG die Bekanntmachungsvorschriften zur Sächsischen Gemeindeordnung kannte und dieser damit bewusst die Regelung zur ausschließlichen

Publikation in öffentlich zugänglichen elektronischen Ausgaben im SächsEGovG getroffen hat, verdrängt § 4 SächsEGovG den § 2 KomBekVO.
Dies bedeutet, dass die KomBekVO eine Kommune nicht daran hindert, eine Satzung auch ausschließlich elektronisch zu verkünden, wenn die Voraussetzungen des § 4 SächsEGovG erfüllt sind und insbesondere die sonst noch notwendigen kommunalrechtlichen Gemeinderatsbeschlüsse gefasst sind.

§ 2 Abs. 1 SächsEGovG – Elektronische Kommunikation und Verschlüsselungsverfahren

§ 2 Abs. 1 SächsEGovG lautet:

»Die staatlichen Behörden und die Träger der Selbstverwaltung müssen auch die elektronische Kommunikation ermöglichen. Beliehene sind von dieser Verpflichtung ausgenommen, soweit die elektronische Kommunikation für die ordnungsgemäße Wahrnehmung ihrer Verwaltungsaufgaben nicht erforderlich ist. Für die elektronische Kommunikation sind Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung zur elektronischen Kommunikation unter grundsätzlicher Anwendung von Verschlüsselungsverfahren im Rahmen der öffentlich-rechtlichen Verwaltungstätigkeit gilt für die Träger der Selbstverwaltung unmittelbar seit Inkrafttreten des Gesetzes am 9. August 2014.

Adressat der Verpflichtung

Zu den Trägern der Selbstverwaltung zählen gemäß Art. 82 Abs. 2 S. 1 SächsVerf die Gemeinden, Landkreise und andere Gemeindeverbände als kommunale Träger der Selbstverwaltung und nach Art. 82 Abs. 3 SächsVerf andere öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen nach Maßgabe der Gesetze als nichtkommunale Träger der Selbstverwaltung.

Daher sind z. B. auch kommunale Verwaltungs- und Zweckverbände oder Verwaltungsgemeinschaften und ferner die Sächsische Anstalt für Kommunale Datenverarbeitung (SAKD) Verpflichtete. Verpflichtete sind insofern auch die kommunalen Eigenbetriebe soweit sie öffentlich-rechtliche Verwaltungstätigkeit wahrnehmen, nicht aber die kommunalen Gesellschaften, da diese sowohl rechtlich als auch organisatorisch aus der Gemeinde ausgegliedert sind. Beliehene, d. h. natürliche oder juristische Personen des Privatrechts, denen durch oder aufgrund eines Gesetzes hoheitliche Befugnisse übertragen wurden, müssen die elektronische Kommunikation nur ermöglichen, wenn es zu ihrer Aufgabenerfüllung erforderlich ist. Ob ein solches Erfordernis besteht, richtet sich nach den jeweils für sie geltenden rechtlichen Bestimmungen, im Wesentlichen nach dem einschlägigen Fachrecht.

Geltungsbereich der Verpflichtung

Die Verpflichtung liegt darin, die elektronische Kommunikation zu ermöglichen, die zur Durchführung öffentlich-rechtlicher Verwaltungstätigkeit erforderlich ist. Damit ist die privatrechtliche Verwaltungstätigkeit der öffentlichen Hand von der Verpflichtung nicht umfasst. Verwaltungstätigkeit umfasst sämtliche Formen des Verwaltungshandelns eines Verwaltungsträgers. Dies betrifft damit nicht nur die Verwaltungstätigkeit, die im Rahmen von Verwaltungsverfahren nach § 1 SächsVwVfZG i. V. m. § 9 VwVfG durchgeführt wird, also die mit Außenwirkung versehene, auf den Antragsteller, den Bürger oder das Wirtschaftsunternehmen gerichtete Verwaltungstätigkeit (Verfahren zum Erlass eines Verwaltungsaktes oder Abschluss eines öffentlich-rechtlichen Vertrages). Auch die Behörden übergreifende Kommunikation, die zur Durchführung von Verwaltungsverfahren erfolgt (z. B. fachaufsicht-

liche Hinweise; Amtshilfeersuchen) muss elektronisch möglich sein. Umfasst ist aber auch die Verwaltungstätigkeit, die zwischen Behörden oder sonstigen öffentlichen Stellen erfolgt und nicht auf die Durchführung eines Verwaltungsverfahrens abzielt oder durch dieses veranlasst ist (z. B. Informationsschreiben; Anfertigen von Gutachten oder Stellungnahmen durch Zuarbeit). Gleiches gilt für die Verwaltungstätigkeit zwischen Behörden und sonstigen öffentlichen Stellen innerhalb einer Verwaltungseinheit, insbesondere in den kreisfreien Städten (z. B. Datenübermittlungen zur Erstellung von Wählerverzeichnissen oder Datenabrufe der Ausländerbehörde bei der Meldebehörde einer kreisfreien Stadt zum internen Datenabgleich).

Inhalt der Verpflichtung

Unter der elektronischen Kommunikation versteht man das Senden und Empfangen von Nachrichten mittels elektronischer Medien. Nicht darunter fällt die Übermittlung von Nachrichten auf Trägermedien, z. B. CD oder DVD, auch wenn die Daten auf den Trägern elektronisch erzeugt sind.

Die Träger der Selbstverwaltung müssen die elektronische Kommunikation ermöglichen. Damit müssen sie die erforderlichen technischen und organisatorischen Voraussetzungen schaffen, um elektronische Kommunikationsvorgänge durchzuführen. Da das Gesetz hierzu keine Standards vorgibt, muss die elektronische Kommunikation zumindest nach den allgemein anerkannten Regeln der Technik erfolgen. Dies sind solche technischen Verfahren und Vorgehensweisen, die in der praktischen Anwendbarkeit erprobt sind und von der Mehrheit der Fachleute anerkannt werden.

Es wird der Stand der Technik für die elektronische Kommunikation empfohlen. Dies ist ein entwickeltes Stadium der technischen Möglichkeiten bei Produkten, Prozessen und Dienstleistungen zu einem bestimmten Zeitpunkt, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung. Es sind zumindest die Verfahren einzusetzen, die einen hohen Verbreitungsgrad in der Bevölkerung haben, also insbesondere E-Mail, ggf. E-Fax und für die behördenübergreifende Kommunikation bei Bedarf auch Video. Eine Wahlmöglichkeit für den Einsatz besteht jedoch zumindest insofern nicht, da nach § 2 Abs. 2 SächsEGovG auch die Übermittlung elektronischer Dokumente (z. B. per E-Mail) ermöglicht werden muss. Auch das Bereithalten elektronischer Formulare und Webanwendungen ermöglicht je nach Art des Verwaltungsverfahrens die elektronische Kommunikation im Sinne des Gesetzes.

Die Träger der Selbstverwaltung müssen – wenn sie selbst elektronische Nachrichten übermitteln – diese grundsätzlich, d. h. in der Regel, verschlüsseln, es sei denn, die jeweilige Verwaltungstätigkeit rechtfertigt davon Ausnahmen (z. B. das Versenden einer Presseinformation oder dieses Handlungsleitfadens). Verschlüsseln bedeutet dabei das Einsetzen eines Verfahrens zum Schutz der Daten vor unbefugter Einsichtnahme oder Veränderung, in dem diese mittels eines entsprechenden Algorithmus in eine nur für den Berechtigten erschließbare Form gebracht werden. Daher müssen in der Kommunikation mit Bürgern, Wirtschaft und anderen Behörden Verschlüsselungsverfahren von den Trägern der Selbstverwaltung zur Nutzung angeboten werden, nicht zuletzt auch deshalb, um verschlüsselte Nachrichten des Betroffenen an die Träger der Selbstverwaltung entschlüsseln zu können. Welches Angebot die Verwaltung dem Betroffenen unterbreitet, d. h. welches Verschlüsselungsverfahren, welche Art und welcher Grad der Verschlüsselung zu verwenden ist, ist Sache der Verwaltung. Die Art und der Grad der Verschlüsselung richten sich nach den Anforderungen, die die konkrete Verwaltungstätigkeit jeweils erfordert. Sofern keine spezialgesetzlichen Vorschriften bestehen, steigen die Anforderungen an die Datensicherheit und damit an die einzusetzenden Verschlüsselungsverfahren je höher der Grad der

Vertraulichkeit der Daten ist. Bei personenbezogenen Daten sind zudem die Anforderungen der einschlägigen Datenschutzgesetze zusätzlich zu beachten. Prioritär einzusetzen sind daher datensichere Verfahren, die einen hohen Verbreitungsgrad in der Bevölkerung haben oder solche, die sich in der sächsischen Verwaltungspraxis in der Kommunikation mit Bürgern oder zwischen Behörden bewährt haben (z. B. Elektronisches Gerichts- und Verwaltungspostfach – EGVP, Secure Mailgateway – SMGW). Die Betroffenen haben aus dem SächsEGovG nur dann keinen Anspruch darauf, dass Träger der Selbstverwaltung die Nachrichten auch verschlüsselt an die Betroffenen übermitteln, wenn es dafür sachlich nachvollziehbare Gründe gibt (z. B. wenn der konkrete Inhalt der Verwaltungstätigkeit keine besondere vertrauliche Übermittlung erfordert). In der Regel ist also zu verschlüsseln. Eine Ausnahme liegt auch dann vor, wenn die Betroffenen ausdrücklich – d. h. nicht nur durch konkludentes Handeln, sondern mit eindeutig abgegebener Erklärung – auf eine Verschlüsselung verzichten.

B Empfehlungen zur Umsetzung

Der Verpflichtung nach § 2 Abs. 1 SächsEGovG wird bereits dann Rechnung getragen, wenn die elektronische Kommunikation über eine E-Mail-Adresse sichergestellt werden kann.

Die Verschlüsselung ist gewährleistet, wenn zumindest für eine E-Mail-Adresse sichergestellt wird, dass ein- und ausgehende Nachrichten übertragen werden und die erforderlichen Informationen (Schlüssel, Bedingungen zur Zugangseröffnung) öffentlich verfügbar sind. Aus der Verpflichtung nach § 2 Abs. 1 SächsEGovG ist zudem abzuleiten, dass für Portale und webbasierte Dienste zum Nachrichten- und Datenaustausch grundsätzlich die Verschlüsselung anzubieten ist. Weitere Hinweise zur Absicherung über TLS / SSL sind in den Ausführungen zu § 13 Abs. 1 SächsEGovG zu finden.

Sofern ein Fachgesetz keine Anforderungen enthält, ist das notwendige Verschlüsselungsverfahren über eine Schutzbedarfsanalyse festzustellen. Dafür können die Empfehlungen des IT-Grundschutzes des BSI herangezogen werden. Wenn im Ergebnis der Analyse ein Schutzbedarf »HOCH« (z. B. Geschäftsgeheimnisse, besonders geschützte Daten gemäß § 4 Abs. 2 SächsDSG) festgestellt wird, empfiehlt das BSI eine Ende-zu-Ende-Verschlüsselung (z. B. OSCI).

Im Übrigen werden über die von den Trägern der Selbstverwaltung mitfinanzierte E-Government-Basiskomponente »Elektronische Signatur und Verschlüsselung« (BaK ESV) auch für die Träger der Selbstverwaltung geeignete zentrale Dienste zur Umsetzung der Verpflichtung nach § 2 Abs. 1 SächsEGovG angeboten. Diese sind, vorbehaltlich der Regelung des § 10 Abs. 2 S. 1 SächsEGovG, der am 1. August 2016 in Kraft tritt, zu nutzen.

Datenschutzrechtlichen Anforderungen werden unter anderem dadurch Rechnung getragen, dass ein zentraler Dienst für verschlüsselte E-Mails (siehe Abschnitt B.2) und ein zentraler Dienst für die OSCI-Kommunikation (siehe Abschnitt B.3) genutzt werden kann.

Die benötigten E-Mail- und SSL-Zertifikate können über die als zentraler Dienst betriebene Sachsen Global CA (siehe Abschnitt Zertifikate) oder andere geeignete Zertifizierungsstellen beschafft werden. Auswahlkriterien zu Zertifizierungsstellen sind im Abschnitt Beantwortung häufig gestellter Fragen zu finden.

B.1 Zertifikate

Zertifikate, die zur S/MIME-E-Mail-Verschlüsselung zum Einsatz kommen, müssen die X509-Zertifikatserweiterung »erweiterte Schlüsselverwendung=emailProtection« enthalten. Die zu schützende E-Mail-Adresse muss im Zertifikatsfeld »Subject« bestätigt sein. Als Mindestanforderung sind Class2-Zertifikate einzusetzen.

Serverzertifikate, die zur SSL/TLS-Verschlüsselung von Webanwendungen zum Einsatz kommen, sollen die X509-Zertifikatserweiterung »erweiterte Schlüsselverwendung= serverAuth« enthalten. Die Zertifikate sollen als CommonName (CN) den qualifizierten Domainnamen (FQDN) enthalten und von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt sein.

Über die Webseite der Sachsen Global CA (SGCA) können geeignete Serverzertifikate zum Einsatz für Datenverarbeitungssysteme und Benutzer(gruppen) beantragt werden. In den Ausführungen zu § 13 Abs. 1 SächsEGovG sind vertiefende Erläuterungen und Anleitungen zu Beantragung und Einsatz von Serverzertifikaten enthalten. E-Mail-Funktionsadressen werden über Organisations- oder Gruppenzertifikate abgesichert.

Zusätzliche Hinweise sind im Abschnitt Beantwortung häufig gestellter Fragen und in der Onlinehilfe der DFN-PKI zu finden. Darüber hinausgehende Anfragen können an die Kontaktadresse der SGCA gerichtet werden.

B.2 Umsetzung der E-Mail-Verschlüsselung

Die Transportverschlüsselung (SSL/TLS) zwischen Sender und Empfänger wird am E-Mail-Client und -Server aktiviert. Kann technisch keine Transportverschlüsselung zum Empfänger umgesetzt werden, muss eine Verschlüsselung des Inhaltes der E-Mail erfolgen. Hierfür ist die Implementierung und Veröffentlichung eines Verschlüsselungszertifikates erforderlich. Als Verschlüsselungsverfahren wird die Inhaltsverschlüsselung (S/MIME / PGP) unabhängig von der (zusätzlichen) Nutzung einer Transportverschlüsselung empfohlen.

Stand der Technik sind zentrale Systeme zur Verschlüsselung (Mail Gateway). Über die BaK ESV kann auf eine Software Landeslizenz für das Gateway Z1 (Hersteller Zertificon) zurückgegriffen werden. Nähere Informationen sind über die Kontaktstellen (siehe Abschnitt B.4) zu erhalten.

Sofern die E-Mail der Behörde über das KDN geroutet wird, sollte der Einsatz eines eigenen Verschlüsselungsgateways aus technischen Gründen nicht in Erwägung gezogen werden. In diesem Fall erfüllt die aktivierte Transportverschlüsselung zwischen Sender und Empfänger im KDN / SVN bereits die Mindestanforderungen einer Verschlüsselung.

Zusätzlich wird die Mandatierung auf dem zentralen Secure Mail Gateway (SMGW) des Freistaates Sachsen empfohlen, da das SMGW für die Nachrichtenübermittlung im Internet die Inhalte auf Anwendungsebene verschlüsselt (Inhaltsverschlüsselung über S/MIME oder PGP). Ist kein Empfängerschlüssel bekannt, wird die Nachricht über ein gesichertes Online-Postfach (SMGW-Messenger) zugestellt. Die Nachrichten werden ein- und ausgehend nach dem Stand der Technik auf Viren gescannt. Nähere Informationen sind über die Kontaktstellen (siehe Abschnitt B.4) zu erhalten.

B.3 Umsetzung OSCI – Elektronisches Gerichts- und Verwaltungspostfach

Das OSCI-Protokoll gewährleistet die Ende-zu-Ende-Verschlüsslung (doppelte Verschlüsselung) und wird damit auch höheren datenschutzrechtlichen Anforderungen gerecht. OSCI ist insbesondere zur Kommunikation in Fachverfahren zwischen Behörden verschiedener Ebenen im Einsatz (z. B. im Pass- und Meldewesen). Mit dem Elektronischen Gerichts- und Verwaltungspostfach (EGVP) wird bundesweit ein OSCI Kommunikationsszenario betrieben, an dem auch Bürger und Unternehmen teilnehmen können.

Das EGVP gewährleistet die rechtssichere und verschlüsselte Kommunikation. Über EGVP tauschen bereits heute über 40.000 Nutzer (Anwälte, Notare, Firmen, Gerichte und Behörden) deutschlandweit Nachrichten aus. EGVP wird in Sachsen bereits von Behörden im Rahmen der Umsetzung der EU-Dienstleistungsrichtlinie oder zur rechtssicheren elektronischen Kommunikation mit der Justiz eingesetzt (elektronischer Rechtsverkehr).

Der technische Hintergrund – die Nachrichtenverschlüsselung und -signatur, die Bereitstellung eines ständig aktualisierten deutschlandweiten Verzeichnisdienstes (SAFE) für alle Teilnehmer, die Fachverfahrensanbindung etc. – wird über ein einheitliches Nachrichtenformat und über die bundesweite OSCI-Infrastruktur sichergestellt. Die BaK ESV betreibt den zentralen sächsischen Intermediär und stellt die OSCI-Postfächer für teilnehmende Behörden zur Verfügung.

Jedem EGVP-Teilnehmer ist technisch eine Rolle zugeordnet. Für Bürger, Berufsträger und Unternehmen (Rolle: Bürger) werden zur Kommunikation mit teilnehmenden Behörden (Rolle: Behörde) kostenfrei ein zentraler OSCI-Postfachdienst, Support und Clientsoftware über die EGVP-Website angeboten. Dort angebotene Downloads sind technische Implementierungen für die Rolle Bürger (EGVP Classic Frontend).

Die Implementierung für Behörden mit erweitertem Funktionsumfang (z. B. EGVP Classic Backend) ist **nicht über die EGVP-Website** erhältlich! Behörden werden durch die jeweils zuständigen Stellen in den Bundesländern betreut. In Sachsen erfolgen die Bereitstellung des OSCI-Postfachs und geeigneter Software sowie der Support über die BaK ESV.

Mit der angebotenen EGVP-Software können verschiedene Einsatzszenarien abgebildet werden. Zusätzliche Funktionen des EGVP sind Automatisierungsmöglichkeiten und die Prüfung übermittelter Dokumente mit qualifizierter elektronischer Signatur (qeS). EGVP erfüllt damit zusätzlich auch die Anforderungen nach § 2 Abs. 2 SächsEGovG.

Neben der zentral gepflegten Kommunikationssoftware EGVP Classic und EGVP Enterprise können zugelassene Drittprodukte eingesetzt werden. In diesem Fall sind die EGVP-Postfächer entsprechend der Namenskonvention Sachsen (Namenskonventionen für EGVP Postfächer) in der Rolle »Behörde« im Verzeichnisdienst zu registrieren.

Zusätzliche Hinweise sind im Abschnitt C und online zu finden:

- Beschreibung des EGVP als Teil der BaK ESV
- Bürger- und allgemeines Informationsportal des EGVP
- Herstellerseite der EGVP-Software

B.4 Kontaktmöglichkeiten

Für Rückfragen zu den Abschnitten B.1 (Zertifikate), B.2 (SMGW) und B.3 (OSCI, EGVP) sind die zuständigen Mitarbeiter im Staatsbetrieb SID erreichbar unter:

Staatsbetrieb Sächsische Informatik Dienste
Fachbereich 3.1 – E-Government- und Querschnittverfahren
Betreuung BaK ESV
Riesaer Straße 7
01129 Dresden
Tel.: 0351 20545-280
E-Mail: esv@sid.sachsen.de

E-Mail-Funktionsadressen für spezifische Anfragen zu den einzelnen Verfahren:
Zu Abschnitt B.1 (Zertifikate, Sachsen Global CA Administration): pki@smi.sachsen.de
Zu Abschnitt B.2 (SMGW, E-Mail-Verschlüsselung): smgw@sid.sachsen.de
Zu Abschnitt B.3 (OSCI, EGVP): esv@sid.sachsen.de

Informationen im Internet: Webseite zur BaK ESV sowie Registrierungsformulare für Dienste der BaK ESV (SMGW, OSCI, EGVP)

C Beantwortung häufig gestellter Fragen

Frage 1: Fordert das SächsEGovG eine Inhalts- oder eine Transportverschlüsselung?

> **Antwort**: Das Gesetz enthält keine näheren Bestimmungen zur Implementierung der Verschlüsselungsverfahren. Sowohl Inhalts- als auch Transportverschlüsselung erfüllen die Anforderung, sofern diese nachweislich auch außerhalb des Wirkungsbereichs der Behörde (z. B. SVN / KDN) wirksam sind.
> So verwendet das SMGW z. B. innerhalb des SVN / KDN die Transportverschlüsselung, außerhalb aber die Inhaltsverschlüsselung.

Frage 2: § 2 Abs. 1 S. 3 SächsEGovG erlaubt begrenzte Ausnahmen von der Anwendung der Verschlüsselung bei der elektronischen Kommunikation. Ist bei Datenübermittlungen zwischen Trägern der Selbstverwaltung untereinander und mit anderen Behörden, die ans SVN / KDN angeschlossen sind, insbesondere für den E-Mail-Verkehr, eine Verschlüsselung notwendig oder sind die Netze sicher genug, dass die Datenübermittlungen wie bisher unverschlüsselt erfolgen können?

> **Antwort**: Mit der NSA-Affäre wurde deutlich, dass auch in internen Netzen mit Zugriffen durch unbefugte Dritte zu rechnen ist – siehe dazu den bekannt gewordenen Angriff auf den Betreiber Belgacom. Es ist daher dringend anzuraten, auch innerhalb der Verwaltungsnetze auf verschlüsselte Übertragung zurückzugreifen.
> So bieten moderne Server dies schon in der Grundkonfiguration an (z. B. der in der Staatsverwaltung standardisierte Server »Exchange 2010«). Die für diese Kommunikation notwendigen Zertifikate sind über die Landes-PKI für alle Teilnehmer am verwaltungsinternen Datenverkehr, staatlich oder kommunal, kostenfrei erhältlich. Es ist daher gerade bei der E-Mail-Kommunikation kaum vorstellbar, in welchen Fällen auf eine Verschlüsselung der Transportstrecke verzichtet werden sollte.

Frage 3: Ändert sich daran etwas, wenn personenbezogene Daten (z. B. Passbilder zwischen Passbehörde und Polizeidienststelle) übermittelt werden?

> **Antwort**: Ja. Bei dieser Klasse von Inhalten ist von einem Schutzbedarf »HOCH« auszugehen. Damit ist es bei diesen Daten unerlässlich, auch die Inhalte durch Verschlüsselung zu sichern, zusätzlich zur Transportverschlüsselung. Der Mehrwert ergibt sich hier am Ende der Transportstrecken, also bei den Empfängern (Ende-zu-Ende-Verschlüsselung). Dies geht über den heutigen Stand (nur Transportverschlüsselung) hinaus.

Frage 4: Wie sind Frage 2 und Frage 3 zu beantworten, wenn die Datenübermittlung innerhalb einer Kommune (z. B. zwischen Ordnungsamt und Meldebehörde) a) im Intranet erfolgt oder b) über das Internet abgewickelt wird (insb. wenn die Behörden in unterschiedlichen Orts- oder Stadtteilen oder Gemeinden ihren Dienstort haben)?

> **Antwort**: Sowohl bei a) als auch bei b) ist von den gleichen Regeln auszugehen, wie unter Frage 2 und Frage 3 aufgeführt.

Frage 5: Welche Verschlüsselungsverfahren, die auch vom Bürger unkompliziert eingesetzt werden können, sind zu empfehlen?

> **Antwort**: Empfohlen werden der Austausch von verschlüsselten Dokumenten im Anhang von E-Mails, S/MIME und PGP zur E-Mail-Verschlüsselung, browserbasierte Zugänge zu verschlüsselten Datei- und Nachrichtenablagen (z. B. per SMGW-Messenger) sowie auch OSCI (z. B. per EGVP), sofern es funktional erforderlich ist.

Frage 6: Was ist der Unterschied zwischen öffentlichem und privatem Schlüssel (Zertifikat)?

> **Antwort**: Der private Schlüssel darf nur dem Zertifikatsinhaber vorliegen und sollte zusätzlich durch ein Kennwort geschützt werden, das nur dem Zertifikatsinhaber bekannt ist. Der öffentliche Schlüssel ist nicht geschützt und muss allen Kommunikationspartnern vorliegen. Beide Schlüssel korrespondieren. Daten werden mit dem öffentlichen Schlüssel für den Zertifikatsinhaber verschlüsselt. Die verschlüsselten Daten können nur mit dem privaten Schlüssel (kennwortgeschützt) entschlüsselt werden.

Frage 7: Wie kann ein externer Kommunikationspartner seinen Schlüssel der Behörde bekannt machen?

> **Antwort**: Die Bekanntmachung von Schlüsseln erfolgt über öffentliche Verzeichnisdienste der Zertifikatsaussteller oder z. B. durch das Senden einer mit dem Schlüssel signierten E-Mail an die Behörde. Bei Eingang einer signierten E-Mail im SMGW wird das der Absenderadresse zugeordnete Zertifikat automatisch im SMGW hinterlegt. Im Antwortfall wendet das SMGW den hinterlegten öffentlichen Schlüssel an.

Frage 8: Wie kann eine Behörde ihren Schlüssel dem externen Kommunikationspartner bekannt machen?

> **Antwort**: Die Bekanntmachung von Schlüsseln erfolgt über öffentliche Verzeichnisdienste der Zertifikatsaussteller oder durch Veröffentlichung auf der Internetseite der Behörde, wie z. B. auf der Webseite Signatur und Verschlüsselung der Landesverwaltung Sachsens.

Frage 9: Können Behörden verschlüsselte Nachrichten nur an Empfänger senden, von denen der Behörde bereits ein Empfängerschlüssel bekannt ist?

> **Antwort**: Empfängerschlüssel werden, wenn diese nicht bereits lokal hinterlegt sind, über öffentliche Verzeichnisdienste gesucht. Ist der Schlüssel veröffentlicht, wird dieser benutzt.
> Wird das SMGW genutzt und kein gültiger Schlüssel zur E-Mail-Adresse des Empfängers gefunden, initiiert das SMGW ein sicheres Webpostfach (SMGW Messenger) für den Empfänger, in das die Nachricht zugestellt wird. Der Zugang der Nachricht sowie Informationen zum Abruf werden dem Empfänger dann in einer separaten Nachricht an sein normales Postfach mitgeteilt.

Frage 10: Kann die Behörde vorab ermitteln, ob für den Empfänger bereits ein Schlüssel bekannt ist?

> **Antwort**: Ja, indem öffentliche Verzeichnisdienste oder lokale Adressdaten abgefragt werden. SMGW-Teilnehmer (Rolle: aktiver Nutzer) können vom System vorab Auskunft erhalten, wie eine Nachricht an einen Empfänger durch das System behandelt werden würde (Steuerbefehl »[INFO]«).

Frage 11: Welche E-Mail-Adresse (Domain-Teil) bekommt der Antragsteller als passiver oder aktiver Nutzer des SMGW?

> **Antwort**: Als aktiver Nutzer wird kein gesonderter Domänenteil vergeben. Die Domäne muss aber über die zentralen Netzdienste geroutet werden. Als passiver Nutzer wird ein sogenanntes Messenger-Postfach mit einer lokalen Domäne erstellt (»beispiel@messenger.lokal«). Im Webmessenger (Webmailer) kann die lokale Adresse »beispiel@messenger.lokal« oder aber auch die zugehörige Mailadresse »beispiel@behörde.de« verwendet werden. Lokale Adressen sind nur innerhalb des SMGW gültig. Das Versenden einer Nachricht an eine nicht registrierte Adresse / Domäne ist von einem passiven Postfach aus nicht möglich.

Frage 12: Was geschieht mit der Original-E-Mail, die im SMGW entschlüsselt und geprüft wurde? Ist diese für den Empfänger der Nachricht noch von Bedeutung?

> **Antwort**: Die entschlüsselte E-Mail wird an den Empfänger weitergeleitet. Die verschlüsselte Original-E-Mail wird auf dem SMGW gelöscht, da sie nicht mehr benötigt wird.

Frage 13: Wie kann eine E-Mail Ende-zu-Ende verschlüsselt werden?

> **Antwort**: Ende-zu-Ende-Verschlüsselung per E-Mail erfordert in jedem Fall den Einsatz von entsprechender Verschlüsselungs-Software (z. B. GnuPG) auf den Rechnern der beteiligten Nutzer (Clients der Sender und Empfänger).

Frage 14: Was ist bei der Auswahl eines Zertifikatsanbieters (Certificate Authority, CA) zu beachten?

> **Antwort**: Grundsätzlich wird der Einsatz der landeseigenen Sachsen Global CA empfohlen. Sollte dennoch eine andere CA genutzt werden, sind u. a. folgende Auswahlkriterien zu prüfen:

1. Ggf. wird bereits vom (Fach-)Verfahren oder von übergreifenden IT-Sicherheitskonzepten eine Mindestanforderung an Zertifizierungsstellen definiert.
2. Der Zertifikatsanbieter soll von unabhängiger Stelle überwacht / zertifiziert sein.
3. Die Wurzelzertifikate sollen bereits vom Hersteller in allen gängigen Betriebssystemen, Internetbrowsern und Mailprogrammen als Vertrauensanker eingebunden sein.
4. Die Identifizierung der Zertifikatsnehmer soll im Minimum neben der Prüfung der Identität (z. B. E-Mail-Adresse, FQDN) eine Überprüfung des Unternehmens beziehungsweise der Organisation (z. B. Domaininhaberschaft) beinhalten. Das entspricht i. A. dem nicht standardisierten Begriff »Class 2-Zertifikat«).

Frage 15: Unter welchen Voraussetzungen kann ein Serverzertifikat der Sachsen Global CA beantragt werden?

Antwort:
1. Die Domain des zu zertifizierenden Webauftrittes (Servers) muss für eine Behörde der sächsischen Landes- oder Kommunalverwaltung registriert sein (Admin-C). Die Prüfung erfolgt online z. B. über DENIC oder InterNIC.
2. Der Sachsen Global CA muss eine Vollmacht zur Ausstellung von Serverzertifikaten für die betreffende Domain vom Domaininhaber (Admin-C) erteilt worden sein (Kontaktadresse: PKI@smi.sachsen.de).
3. Zertifikatsanträge sind durch den Verantwortlichen der Behörde einzureichen.
4. Mit der Zertifikatsbeantragung werden die Zertifizierungsrichtlinien der DFN-PKI Policy (Global) akzeptiert.

Frage 16: Stellt die Sachsen Global CA Wildcard-Zertifikate für die SSL-Verschlüsselung aller Server oder Webanwendungen einer Domäne aus?

Antwort: Nein. Es gibt jedoch die Möglichkeit, mehrere zusammengehörige Domainnamen in einem Zertifikat zusammenzufassen (SAN-Zertifikate).

Frage 17: Welche Zertifikatsprofile sind in der Sachsen Global CA implementiert?

Antwort: Die Website der DFN-PKI bietet eine Übersicht zu den Zertifikatprofilen.

Frage 18: Unter welchen Voraussetzungen kann ein Nutzerzertifikat der Sachsen Global CA beantragt werden?

Antwort:
1. Der Nutzer / die Nutzergruppe muss der Landes- oder Kommunalverwaltung Sachsens zugeordnet sein (Prüfung Organisationseinheit / Abteilung).
2. Mit der Zertifikatsbeantragung werden die Zertifizierungsrichtlinien der DFN-PKI Policy (Global) akzeptiert.

Frage 19: Was kostet ein Zertifikat?

Antwort: Für sächsische Behörden und Kommunen sind die Zertifikate der Sachsen Global CA ohne Zusatzkosten erhältlich. Zertifikate anderer Anbieter sind in der Regel kostenpflichtig. E-Mail-Zertifikate gibt es z. B. ab ca. 20 € pro Jahr, Serverzertifikate ab ca. 200 € pro Jahr (jeweils Class2, deutscher Anbieter).

Frage 20: Was ist bei der Beantragung von Zertifikaten für Umlautdomains bei der Sachsen Global CA zu beachten?

> **Antwort**: Bei der Beantragung ist die IDNA-Notation (Internationalizing Domain Names in Applications) zu nutzen. Die Sachsen Global CA ist in der Lage, IDNA-konvertierte Domainnamen zu verarbeiten.

Frage 21: Welche Client-Zertifikate können für OSCI (EGVP) eingesetzt werden?

> **Antwort**: Es bestehen keine organisatorischen Anforderungen. Technisch ist ein x509.V3-Zertifikat mit den Schlüsselverwendungen Signatur und Verschlüsselung erforderlich.
> Im EGVP können geeignete Clientzertifikate selbst erstellt werden. Für die EGVP Rolle »Behörde« erfolgt eine initiale Prüfung der Identität (Postfachregistrierung).

§ 2 Abs. 2 SächsEGovG – Zugangseröffnung für Dokumente mit qualifiziert elektronischer Signatur

§ 2 Abs. 2 S. 1 SächsEGovG lautet:

»Die Übermittlung elektronischer Dokumente unter Wahrung der für den Freistaat Sachsen verbindlichen bundesrechtlichen Voraussetzungen in

1. § 3a Abs. 2 des Verwaltungsverfahrensgesetzes (VwVfG) in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 3 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749, 2753) geändert worden ist, in der am 8. August 2014 geltenden Fassung,
2. § 36a Abs. 2 des Ersten Buches Sozialgesetzbuch (SGB I) – Allgemeiner Teil – (Artikel 1 des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), das zuletzt durch Artikel 10 des Gesetzes vom 19. Oktober 2013 (BGBl. I S. 3836, 3848) geändert worden ist, in der am 8. August 2014 geltenden Fassung, und
3. § 87a Abs. 3, 4 und 6 der Abgabenordnung (AO) in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 13 des Gesetzes vom 18. Dezember 2013 (BGBl. I S. 4318, 4333) geändert worden ist, in der am 8. August 2014 geltenden Fassung,

für die Ersetzung der Schriftform ist durch die staatlichen Behörden und die Träger der Selbstverwaltung im Rahmen der Kommunikation nach Absatz 1 unter dem Vorbehalt der Bereitstellung von Haushaltsmitteln für die Umsetzung zu ermöglichen, soweit nicht wichtige Gründe entgegenstehen.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung, Schriftform ersetzende elektronische Dokumente senden und empfangen zu können, tritt zwei Jahre nach Verkündung des SächsEGovG in Kraft (vgl. Art. 3 Abs. 2 Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen und zur Änderung des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung). Sie gilt damit für die Träger der Selbstverwaltung (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG) ab dem 1. August 2016.

Davon unberührt bleibt die schon seit dem 1. Juli 2014 bestehende Verpflichtung aus § 2 Abs. 1 E-Government-Gesetz des Bundes, den Zugang für die Übermittlung elektronischer Dokumente zu eröffnen (d. h. den Empfang entsprechender Nachrichten zu ermöglichen), die mit einer qualifizierten elektronischen Signatur (qeS) versehen sind, wenn Bundesrecht ausgeführt wird. Gleiches gilt (auch für den Weg der Übermittlung von Nachrichten), wenn durch Rechtsvorschrift angeordnet ist, dass ein Verwaltungsverfahren über eine einheitliche Stelle abgewickelt werden kann und die Abwicklung in elektronischer Form verlangt wird (vgl. §§ 71a, 71 d, 71 e VwVfG). Zur Umsetzung dieser Verpflichtungen kann ebenfalls auf die Empfehlungen unter Abschnitt Empfehlungen zur Umsetzung zurückgegriffen werden.

Unberührt bleibt auch die Verpflichtung der Verwaltung, Anträge und Anzeigen in Ausführung von Bundes- oder Landesrecht empfangen zu können, die nach Maßgabe des De-Mail-

Gesetzes schriftformersetzend übermittelt werden. Gleichfalls unberührt bleibt diese Verpflichtung beim Empfang elektronischer Formulare, die über öffentlich zugängliche Netze zur Verfügung gestellt werden und die mit Hilfe des sicheren Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Abs. 5 des Aufenthaltsgesetzes schriftformersetzend ausgefüllt werden. Voraussetzung ist hier jedoch derzeit noch die Zugangseröffnung nach § 1 S. 1 SächsVwVfZG i. V. m. § 3a Abs. 1 VwVfG (vgl. § 1 Abs. 1 bis 3 VwVfG i. V. m. § 1 S. 1 SächsVwVfZG, § 19 Abs. 1 SächsEGovG).

Erst mit Inkrafttreten von § 2 Abs. 2 SächsEGovG müssen auch elektronische Dokumente mit Hilfe von De-Mail oder den neuen Personalausweis schriftformersetzend empfangen und ggf. auch mittels De-Mail übermittelt werden können. Damit haben die Behörden des Freistaates Sachsen und die Träger der Selbstverwaltung bis zum 1. August 2016 Zeit, diese neuen schriftformersetzenden Verfahren in den Vollzug einzuführen.

Hierzu werden in späteren Versionen des Handlungsleitfadens (ab 2016) Ausführungen enthalten sein.

Geltungsbereich der Verpflichtung

Die Verpflichtung, im Rahmen der Kommunikation nach § 2 Abs. 1 SächsEGovG (siehe dazu Erläuterungen zu § 2 Abs. 1 SächsEGovG), Schriftform ersetzende Dokumente sowohl bei der Durchführung von Verwaltungs- und Sozialverfahren, in Verfahren nach der Abgabenordnung als auch beim sonstigen Verwaltungshandeln, sofern dort ein Schriftformerfordernis durch Rechtsvorschrift (Gesetz, Verordnung, Verwaltungsvorschrift) vorgeschrieben oder angeordnet ist, verarbeiten zu können, gilt nicht nur zwischen staatlichen Behörden und den Trägern der Selbstverwaltung. Sie gilt auch zwischen den Trägern der Selbstverwaltung selbst und zwischen Behörden oder sonstigen öffentlichen Stellen eines Trägers der Selbstverwaltung, insbesondere in den Fällen, in denen das die Schriftform ersetzende Dokument zur Durchführung eines öffentlich-rechtlichen Verfahrens weitergeleitet werden muss.

Inhalt der Verpflichtung

Schriftform ersetzende elektronische Dokumente sind solche, die die Voraussetzungen des § 3a Abs. 2 VwVfG, § 36a Abs. 2 SGB I oder § 87a Abs. 3, 4 und 6 AO erfüllen, z. B. ein elektronisches Dokument mit qeS.

Im Übrigen können weitere Schriftform ersetzende Verfahren durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates erlassen werden, die dann jeweils zwei Jahre nach Inkrafttreten der Bundesnorm auch in Sachsen verbindlich werden (vgl. dazu § 2 Abs. 2 S. 2 SächsEGovG).

Für die Umsetzung der Verpflichtung bestehen folgende Vorbehalte:

Aufgrund des **Haushaltsvorbehaltes** in § 2 Abs. 2 S. 1 SächsEGovG wirkt die Verpflichtung erst, wenn die Träger der Selbstverwaltung die notwendigen Mittel zur Verfügung stellen, um die Schriftform ersetzenden Verfahren einzusetzen.

Da für die Umsetzung der Schriftform ersetzenden Verfahren im Sinne des SächsEGovG eine Erweiterung der bisher gemeinsam von Kommunen und Staat finanzierten Basiskomponente »Elektronische Signatur und Verschlüsselung« geplant ist, die nicht nur den staatlichen Behörden, sondern auch den Trägern der Selbstverwaltung zur Verfügung gestellt werden soll, werden für die Träger der Selbstverwaltung im Wesentlichen voraussichtlich nur die Sach- und Personalkosten für den Anschluss und die Pflege der lokalen Komponenten an die Basisplattform haushaltsrelevant.

Auch nach der zweijährigen Übergangsfrist können jedoch die Behörden und Verwaltungseinrichtungen im Freistaat Sachsen nach § 2 Abs. 2 S. 1 SächsEGovG auf die Ermöglichung der Übermittlung elektronischer Dokumente über schriftformersetzende Verfahren verzichten, **soweit und solange wichtige Gründe hierfür vorliegen**. Diese Ausnahme wird insbesondere in der Übergangszeit nach der Einführung neuer schriftformsetzender Verfahren eingreifen, da nicht alle Träger der Selbstverwaltung diese neuen Verfahren innerhalb der zeitlichen Vorgaben werden umsetzen können.

Der Freistaat Sachsen beabsichtigt vor diesem Hintergrund die Nutzung der neuen schriftformersetzenden Verfahren für die Träger der Selbstverwaltung, insbesondere für die sächsischen Kommunen zu erleichtern. Dabei kommt neben der technischen Unterstützung über Basiskomponenten für die Nutzung von De-Mail z. B. auch die Beantragung gemeinsamer Berechtigungszertifikate zur Nutzung des elektronischen Identitätsnachweises gemäß § 2 Abs. 4, § 18 Abs. 4, § 21 Personalausweisgesetz (PAuswG) und § 78 Abs. 5 S. 1 Aufenthaltsgesetz (AufenthG) für den Freistaat Sachsen und die sächsischen Kommunen in Betracht. Soweit und solange aus technischen oder rechtlichen Gründen eine derartige Zusammenarbeit für einzelne schriftformersetzende IT-Verfahren nicht möglich ist, werden grundsätzlich wichtige Gründe i. S. v. § 2 Abs. 2 S. 1 SächsEGovG einer fristgerechten Einhaltung der Verpflichtung entgegenstehen. Dies gilt insbesondere, so lange aufgrund möglicherweise nicht rechtzeitig bereitgestellter Haushaltsmittel die Umsetzung noch nicht verwirklicht wurde.

Die Basiskomponente »Elektronische Signatur und Verschlüsselung« ist zudem von der zwischen dem Freistaat Sachsen und den kommunalen Landesverbänden am 20. August 2014 abgeschlossenen Vereinbarung zur Mitnutzung der E-Government-Basiskomponenten durch die sächsischen Kommunalverwaltungen (Nutzungsvereinbarung) erfasst und wird daher den Kommunen durch den Freistaat Sachsen (in Übereinstimmung mit § 14 Abs. 1 S. 1 SächsEGovG) zur Verfügung gestellt. Nach § 14 Abs. 1 S. 1 SächsEGovG kann diese Basiskomponente darüber hinaus auch den nichtkommunalen Trägern der Selbstverwaltung zur Verfügung gestellt werden.

B Empfehlungen zur Umsetzung

Die qualifizierte elektronische Signatur (qeS) ist – wie im Abschnitt Erläuterung der Verpflichtung erläutert – der handschriftlichen Unterschrift gleichgestellt.

Für den Umgang mit der qeS gelten technische, rechtliche und organisatorische Vorgaben (Technische Richtlinien, Verordnungen). Ein Signaturworkflow (Lebenszyklus) umfasst:

- Signaturerstellung (Unterschreiben),
- Signaturprüfung (Kontrolle / Akzeptanz) und
- Signaturerhaltung (beweiswerthaltige Speicherung).

Ein Zugang für qeS nach Anforderung umfasst die Signaturprüfung und ggf. die Signaturerhaltung sowie organisatorische Rahmenbedingungen. Die Signaturerstellung zählt explizit nicht zur Zugangseröffnung. Will man aber Dokumente z. B. an einen Bürger elektronisch versenden und muss diese von Rechts wegen unterschreiben (d. h. die Schriftform ist angeordnet) so muss man auch eine solche Signatur erstellen können. Dazu erfolgen Ausführungen in einer späteren Version dieses Handlungsleitfadens, da eine Verpflichtung aus dem SächsEGovG hierfür in Sachsen erst ab dem 1. August 2016 gilt.

Vor Weiterverarbeitung eines Dokuments mit qeS ist es aus Gründen der Datensicherheit (Erkennung von Manipulationen) geboten, die Integrität (mathematische Signaturprüfung), besser auch die Authentizität (Onlineprüfung des Zertifikates des Unterzeichners) des Dokuments sicherzustellen. Beide Prüfungen sind in bestätigten Signatur-Software-Produkten miteinander verknüpft.

Die Notwendigkeit zur Signaturprüfung (Identitätsprüfung) besteht nur im Rahmen von Verfahren, bei denen die qeS als Schriftformersatz zum Einsatz kommt und liegt im Rahmen des pflichtgemäßen Ermessens der Behörde.

Nach gegenwärtigem Kenntnisstand umfasst die Zugangseröffnung für Dokumente mit qeS im Minimum folgende Veröffentlichungspflichten aus § 2 Abs. 2 S. 3 SächsEGovG:

- dem Bürger wird die qeS-Adresse / das qeS-Verfahren bekanntgegeben (z. B. über die Webseite der Behörde oder der Einrichtung oder über eine entsprechende Ergänzung in der E-Mail-Signatur),
- dem Bürger werden eventuelle Formatvorgaben bekannt gegeben (z. B. Dateiformate),

sowie folgende Prozessschritte:

- beim Eingang der Nachricht oder des signierten Dokuments wird durch die Behörde mit zugelassenen oder herstellererklärten Signaturanwendungskomponenten (SAK) gemäß Signaturgesetz / Signaturverordnung die Integrität und Authentizität geprüft,
- die Weiterverarbeitung erfolgt nur nach dokumentierter erfolgreicher Prüfung,
- die Ablage erfolgt in einem beweiswerterhaltenden Speicher oder das Dokument erfährt eine regelmäßige Übersignatur.

B.1 Aktueller Stand der Umsetzung

Mit Umsetzung der EU-Dienstleistungsrichtlinie (RL 2006/123/EG) wurden durch sächsische Behörden elektronische Zugänge z. B. für verschlüsselte Nachrichten (E-Mail, EGVP) und für die qeS eröffnet. Im Rahmen der Umsetzung wurden die Angebote der E-Government-Basiskomponente Elektronische Signatur und Verschlüsselung (BaK ESV) dahingehend erweitert, dass der qeS-Workflow auf der Basis der BaK ESV landeseinheitlich umgesetzt werden kann.

Im Speziellen wurden die Dienste:

- Signaturerstellungsdienst (Software und Hardware),
- Signaturprüfdienst (Software) und
- Signaturspeicherdienst (Software)

produktiv implementiert oder als Testszenario (Signaturspeicherdienst) aufgebaut. Sie stehen damit allen Trägern der Selbstverwaltung sofort zur Verfügung (einzelne Dienste nur im SVN / KDN verfügbar).

B.2 Technische Implementierung

B.2.1 Signaturerstellungsdienst

Signaturerstellungsdienste werden in dieser Version des Handlungsleitfadens nicht betrachtet, da in Sachsen erst ab 1. August 2016 das Versenden elektronisch signierter Dokumente zu ermöglichen ist. Bereits jetzt können aber über die BaK ESV bestätigte Softwareprodukte und -dienste zur Signaturerstellung von allen Trägern der Selbstverwaltung genutzt werden.

B.2.2 Signaturprüfdienst

Die BaK ESV bietet einen zentralen Signaturprüfdienst über die Governikus Service Components Webservice-Schnittstelle an. Dieser Dienst wird bereits jetzt landeseinheitlich von verschiedenen Clientsystemen genutzt. Er stellt durch zentrale Konfiguration und Pflege eine konsistente Integritäts- und Authentizitätsprüfung sicher. Typische Anwendungsbereiche sind EGVP, Secure Mail Gateway, EDAS (SLT), Governikus Signer (VIS.SAX, EU-DLR Behörden).

Folgende Verfahren zur Signaturprüfung können im Einzelnen genutzt werden, wobei als Minimalvariante auf die Ausführungen im Abschnitt Beschreibung eines minimalen Einsatzszenarios (Signaturprüfdienst) verwiesen wird.

Variante 1: Governikus Signer (manuelle Prüfung)

- Als Arbeitsplatzinstallation (Einzelinstallation, z. B. EU-DLR Behörden)
- Als Arbeitsplatzinstallation (über Software-Verteilung, z. B. Elektronischer Rechtsverkehr)
- Als Funktion in Fachverfahrenssoftware integriert (z. B. VIS.SAX)
- Grundeinstellungen sind lokal konfigurierbar (z. B. Prüfprotokoll als PDF / HTML)
- Der Governikus Signer agiert als Client gegenüber dem zentralen Prüfdienst Sachsen.

Variante 2: Governikus WebVerifier (manuelle Prüfung)

- Zugriff über eine grafische Benutzeroberfläche auf eine Webadresse: Testbeispiel
- Zur Zeit nur ein Standardmandant
- Pro Mandant sind Grundeinstellungen konfigurierbar (z. B. Prüfprotokoll als PDF / HTML)
- Der Governikus WebVerifier agiert als Client gegenüber dem zentralen Prüfdienst Sachsen.

Variante 3: Governikus Verification Service (Webservice für automatische Prüfung):

- Mandatierung (sichere Verbindung zu Prüfdienst) erforderlich, z. B. EDAS (SLT) oder SMGW (BaK ESV)
- Pro Mandant sind Grundeinstellungen konfigurierbar (z. B. Prüfprotokoll als PDF / HTML)

- Der Governikus Verification Service agiert als Client gegenüber dem zentralen Prüfdienst Sachsen.

Variante 4: E-Mail-Anbindung an das SMGW (Secure Mail Gateway als berechtigter Empfänger)

- Eingehende E-Mail wird über SMGW geroutet
- SMGW leitet signierte PDF-Anhänge zur Prüfung an den zentralen Prüfdienst weiter und fügt das Ergebnis (Prüfprotokoll) der intern zugestellten E-Mail bei (Behörde muss nur bei einer ungültigen Prüfung eine manuelle Nachprüfung anstoßen, z. B. über Governikus Signer oder über Governikus WebVerifier).
- Zusätzlich kann der SMGW-Zugang genutzt werden, um verschlüsselte E-Mails zu senden und zu empfangen
- Das SMGW als zentrale Mailinfrastruktur des SVN / KDN agiert als Client gegenüber dem zentralen Prüfdienst Sachsen.

Variante 5: Formularserver (Websigner/Verification Engine)

- Die Basiskomponente Formularservice (BaK FS) hat grundsätzlich Formulare mit qeS-Fähigkeit im Portfolio.
- Eingereichte qeS-Formulare werden durch einen Baustein im Gateway (Verification Engine) verarbeitet und zur Prüfung an den zentralen Dienst gesendet
- Formularserver und Formulargateway der BaK FS agieren als Client gegenüber dem zentralen Prüfdienst Sachsen.

Variante 6: Eröffnung eines OSCI-Postfachs (mit EGVP)

- Anhänge einer EGVP-Nachricht werden automatisch im EGVP Client geprüft
- Ein Prüfprotokoll wird zur Verfügung gestellt (auch als XML)
- EGVP kann auch als zentrale Komponente im Rechenzentrumsbetrieb genutzt (EGVP Enterprise) und an Fachverfahren angebunden werden
- EGVP agiert als Client gegenüber dem zentralen Prüfdienst Sachsen.

B.2.3 Signaturspeicherdienst

Der Signaturspeicherdienst befasst sich u. a. mit der Beweiswerterhaltung von qualifiziert signierten Dokumenten. Die Technische Richtlinie 03125 des BSI (TR-ESOR) merkt zur Beweiswerterhaltung an, »dass jedes elektronische Dokument als Beweismittel gemäß § 286 ZPO im Rahmen der freien Beweiswürdigung fungieren kann. Davon zu unterscheiden ist der erleichterte Anscheinsbeweis nach § 371a ZPO. Um diesen zu führen, sind nach der heutigen Rechtslage ggf. besondere Maßnahmen (wie z. B. eine Neusignierung nach § 17 Signaturverordnung, SigV) erforderlich. Werden diese Maßnahmen unterlassen, verliert ein Dokument dadurch nicht jeglichen Beweiswert, sondern es entfällt lediglich die besondere Beweiskraft nach § 371a ZPO. Der Begriff Beweiswerterhalt in dieser Richtlinie ist in diesem Sinne zu verstehen und zu interpretieren.«

Im Rahmen der **manuellen Beweiswerterhaltung** kann der Beweiswert einer Signatur grundsätzlich durch Übersignatur mit gleichem Signaturniveau erreicht werden (§ 17 SigV). Dafür ist technisch mindestens ein Signaturarbeitsplatz (Leser + Signaturkarte + Signatur-

software) erforderlich (Signaturdienst). Dafür empfohlene qualifizierte Zeitstempel können über die Webservice-Schnittstellen der Governikus Service Components abgerufen werden (Aussteller: Deutsche Rentenversicherung). Dieses Szenario ist jedoch sehr aufwendig und deckt nicht alle Bedrohungsszenarien ab (z. B. erfolgreiche Angriffe auf Kryptoalgorithmen). Die manuelle Beweiswerterhaltung wird daher nicht zur breiten Anwendung empfohlen.

Die **automatisierte Beweiswerterhaltung** basiert ebenfalls auf der Übersignatur mit qualifizierten Zeitstempeln entsprechend (§ 17 SigV). Der empfohlene Standard zur automatisierten Beweiswerterhaltung kryptographisch signierter Dokumente ist in der Technischen Richtlinie 03125 des BSI (TR-ESOR) beschrieben. Vornehmlicher Anwendungsbereich dieser Richtlinie sind die Bundesbehörden im Rahmen der gesetzlichen Aufbewahrungspflichten. Darüber hinaus besitzt die Richtlinie empfehlenden Charakter. Ein TR-ESOR-konformes Testsystem wird innerhalb der BaK ESV betrieben. Der Zugriff erfolgt mandantenbezogen über standardisierte Webservices oder über Testclients. Qualifizierte Zeitstempel werden automatisiert über die Webservice-Schnittstellen der Governikus Service Components abgerufen (Aussteller: Deutsche Rentenversicherung). Die automatisierte Beweiswerterhaltung befindet sich derzeit im Testbetrieb. Ein produktiver Einsatz wird geprüft. Im Übrigen siehe FAQ Nr. 4 zu § 2 Abs. 2 SächsEGovG.

B.3 Beschreibung eines minimalen Einsatzszenarios (Signaturprüfdienst)

Zur Umsetzung eines minimalen Szenarios für den Einsatz des Signaturprüfdienstes in einer Behörde mit maximal 1.000 Anwendungsfällen (Signaturprüfungen) pro Monat wird folgendes Vorgehen empfohlen:

- Entscheidung für einen manuellen Signaturprüfdienst (Einzelsignaturprüfung)
- Auswahl einer zentralen E-Mail-Adresse, über den generell der Zugang von Dokumenten mit qeS in die Behörde erfolgen soll.
- Treffen organisatorischer Regelungen (z. B. Vertretungen, Weiterleitungen, Postfachstrukturen)
- Schulung von Personal
- Installation des Governikus Signer an einem einzelnen Arbeitsplatz (Variante 1)
- Test der erfolgreichen Wirkung der getroffenen organisatorischen und technischen Maßnahmen
- Zugangseröffnung durch öffentliche Bekanntgabe (z. B. auf der Website der Behörde und in den E-Mail-Signaturen der Mitarbeiter).

Dieses Vorgehen sollte als Einstieg verstanden werden. Schrittweise kann das Minimalszenario erweitert werden, indem z. B. weitere E-Mail-Adressen veröffentlicht werden, insbesondere für Sachgebiete oder Ämter mit hohem Aufkommen an Dokumenten mit qeS und weitere Arbeitsplätze zur Signaturprüfung eingerichtet werden.

Bei höherem Aufkommen sollten automatisierte Prüfverfahren zur Anwendung kommen (Varianten 3 bis 6).

Sobald externe Dienstleister in die Signaturprüfung von Dokumenten einbezogen werden (Varianten 2 bis 6), sind vertragliche Regelungen mit diesen Dienstleistern zur »Datenverarbeitung im Auftrag« erforderlich. Dies gilt nicht bei ausschließlicher externer Abfrage von Sperrlisteninformationen nach § 15 Abs. 3 SigV.

B.4 Erweiterungen

Es bestehen verpflichtende Anforderungen zur Umsetzung der beweiswerterhaltenden Speicherung nur für Bundesbehörden gemäß Technischer Richtlinie 03125 des BSI (TR-ESOR). Sie hat für andere Behörden empfehlenden Charakter.

In Verbindung mit weiteren Anforderungsquellen (revisionssichere Speicherung, De-Mail) muss noch geprüft werden, ob, und wenn ja, wie ein mandantenfähiges Speichersystem nach TR-ESOR im SVN / KDN aufzubauen und in den Produktivbetrieb zu überführen ist. Teile der bestehenden Infrastruktur können genutzt werden (Governikus Service Components).

B.5 Weitere Informationen

Im Anhang zu diesem Handlungsleitfaden sind weitere Informationen zum Thema elektronische Signatur enthalten:

- Präsentationsfolien eines AK-ITEG-Workshops zum Zugang für qualifiziert elektronisch signierte Dokumente
- Ausarbeitung zu elektronischen Signaturen des Landratsamtes Bautzen

B.6 Kontaktmöglichkeiten

Für Rückfragen steht die Betreuung der BaK ESV zur Verfügung.

Staatsbetrieb Sächsische Informatik Dienste
Fachbereich 3.1 | E-Government- und Querschnittverfahren
Betreuung BaK ESV
Riesaer Straße 7
01129 Dresden
Tel.: 0351 20545-280
E-Mail: esv@sid.sachsen.de

C Beantwortung häufig gestellter Fragen

Frage 1: Können die im Rahmen der Umsetzung der EU-Dienstleistungsrichtlinie eingerichteten technischen Verfahren zur Signaturprüfung auch für andere Verwaltungsverfahren eingesetzt werden?

> **Antwort**: Ja.

Frage 2: Wie ist mit Dokumenten umzugehen, die mit einer ausländischen Signatur versehen sind?

> **Antwort**: In diesen Fällen ist eine Überprüfung des eingehenden Zertifikats von Hand mit Hilfe der so genannten »Trusted Lists« der EU-Mitgliedstaaten erforderlich. Hierbei handelt es sich um ein Verzeichnis, aus dem sämtliche beaufsichtigte / akkreditierte, d. h. vertrauenswürdige Zertifizierungsdiensteanbieter des jeweiligen Mitgliedsstaates, die von ihnen angebotenen Dienste sowie einige technische Details (z. B. hinsichtlich der Erzeugung von Zertifikaten) hervorgehen. Zukünftig können Software-Unternehmen Verifizierer entwickeln, in die die Informationen der Trusted

Lists eingepflegt werden. Dies wird langfristig die elektronische Überprüfung von Signaturen und dazugehörigen Zertifikaten aus dem europäischen Ausland ermöglichen.

Frage 3: Wann gilt eine Signatur als geprüft mit positivem Ergebnis. Kann es z. B. auch ein positives Prüfergebnis geben, wenn ein Dritter das einzureichende Dokument signiert hat?

Antwort: Es wird auf das Anwenderhandbuch Governikus Prüfprotokoll verwiesen. Ein positives Prüfergebnis wird grün angezeigt: »Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis«.
Geprüft werden kann jedoch nur die vorhandene Signatur zum Dokument. Unterschreiben muss immer der Zuständige und nicht ein Dritter.

Frage 4: Wie ist praktisch mit qeS-signierten und geprüften Dateien in der weiteren Aktendokumentation (DMS, VBS) umzugehen, um auch langfristig die erfolgreiche Signaturprüfung zu dokumentieren?

Antwort: Im Kern geht es um die Fragestellung, wie qualifizierte elektronische Signaturen (qeS) im Rahmen elektronischer Aktenführung zu speichern und aufzubewahren sind. Es ist einerseits denkbar, die qeS zu speichern und im Falle, dass ihre Gültigkeit zu erlöschen droht, gemäß § 17 SigV über zu signieren. Durch dieses Verfahren wird die qeS dauerhaft beweiswerterhaltend (i. S. v. § 371a ZPO) aufbewahrt.
Alternativ wäre die qeS zu prüfen. Dokument und Prüfprotokoll wären in geschützter Umgebung, z. B. in einem DMS oder VBS durch Zugriffsrechte gesichert, abzulegen. Eine spätere Prüfung der Signatur ist dann nicht mehr möglich.
Insofern muss – je nach Verwaltungsverfahren – durch die Behörde selbst entschieden werden, welche Beweiskraft dem Dokument aus ihrer Sicht zukommen soll.
Viele rechtliche und auch technische Fragen sind in diesem Bereich noch ungeklärt. Es wird erforderlich sein, die Fragestellung nach Ablauf eines gewissen Zeitraums im Lichte neuer praktischer und rechtlicher Erfahrungen erneut zu prüfen. Zum Begriff der »Beweiswerterhaltung« wird auf den »Signaturspeicherdienst« im Abschnitt B verwiesen. Zu den technischen Möglichkeiten wird auf die »Automatisierte Beweiswerterhaltung« im Abschnitt B verwiesen.

Frage 5: Wie muss mit einem Dokument umgegangen werden, das zwar mit einer qeS signiert wurde, für das aber die Schriftform überhaupt nicht erforderlich ist?

Antwort: Eine Verpflichtung zur Prüfung einer unaufgefordert übersandten qeS besteht nicht.

§ 3 SächsEGovG – Elektronische Zahlungsverfahren

§ 3 SächsEGovG lautet:

»Die staatlichen Behörden und die Träger der Selbstverwaltung müssen elektronische Zahlungen ermöglichen.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung, bei der öffentlich-rechtlichen Verwaltungstätigkeit natürlichen oder juristischen Personen elektronische Zahlungen zu ermöglichen, tritt unmittelbar nach Verkündung des SächsEGovG in Kraft. Sie gilt für die Träger der Selbstverwaltung (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG) seit dem 9. August 2014.

Inhalt der Verpflichtung

§ 3 SächsEGovG schreibt lediglich das Angebot (zumindest) eines elektronischen Zahlungsverfahrens vor, ohne dieses näher zu definieren. Diese allgemeine Pflicht ist schon erfüllt, wenn z. B. die Überweisung als ein auch elektronisch nutzbares Zahlungsverfahren angeboten wird. Unter Berücksichtigung der konkreten in § 3 SächsEGovG enthaltenen Vorgaben bleibt es den Kommunen darüber hinaus aber unbenommen, weitere elektronische Bezahlverfahren z. B. unter Verwendung von Kartenlesegeräten einzusetzen, um insbesondere Verwaltungskosten und sonstige Zahlungsverpflichtungen vor Ort auch elektronisch zu begleichen und damit insbesondere die Bürgerservices zu verbessern (siehe Empfehlungen zur Umsetzung unter Abschnitt Weitere Umsetzungsmöglichkeiten).

Die Regelung tritt ergänzend neben die Vorgaben aus § 4 i. V. m. § 1 Abs. 2 E-Government-Gesetz des Bundes, wonach die staatlichen Behörden und die Träger der Selbstverwaltung, wenn sie Bundesrecht ausführen, seit dem 1. August 2013 verpflichtet sind, die Einzahlung von Gebühren und die Begleichung sonstiger Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen und hinreichend sicheren Zahlungsverfahren zu ermöglichen. Aufgrund der in § 3 SächsEGovG enthaltenen Vorgaben gilt diese Verpflichtung nicht nur bei der Ausführung von Bundesrecht, sondern nunmehr einheitlich für die gesamte öffentlich-rechtliche Verwaltungstätigkeit der staatlichen Behörden und Träger der Selbstverwaltung. Daher müssen Bürger und Unternehmen, die den Kontakt zur sächsischen Verwaltung suchen, nicht prüfen, ob im konkreten Verwaltungsvorgang Bundes- oder Landesrecht ausgeführt wird, sondern können sicher sein, dass in jedem Fall die bargeldlose Zahlung, insbesondere unter Nutzung ihrer Online-Banking-Dienste möglich ist. Durch die flächendeckende Einführung der elektronischen Zahlungsmöglichkeiten im Freistaat Sachsen werden mit der Absicherung elektronischer Zahlungsverfahren durchgängig medienbruchfreie, IT-unterstützte Verwaltungsprozesse ermöglicht, die mit signifikanten Erleichterungen und Beschleunigungen sowohl für Bürger und Unternehmen, als auch für die betroffenen Verwaltungseinheiten selbst einhergehen werden.

Ergänzt wird die Regelung durch die in § 18 Abs. 3 S. 1 Nr. 7 SächsEGovG enthaltene Kompetenz des IT-Kooperationsrates, Empfehlungen abzugeben für elektronische Zahlungsverfahren, die im gesamten Freistaat Sachsen von staatlichen Behörden und Kommunen gleichermaßen angeboten werden sollen.

B Empfehlungen zur Umsetzung

Zur Umsetzung der gesetzlichen Verpflichtung ist zunächst zu prüfen, ob es im eigenen Zuständigkeitsbereich gebührenpflichtige Geschäftsfälle gibt, die aufgrund existierender Vorschriften nur per Barzahlung abgewickelt werden dürfen. Sofern solche Geschäftsfälle identifiziert wurden, sind die hierfür geltenden Rechtsgrundlagen (z. B. kommunale Satzung; Dienstanweisungen) zu prüfen und die Vorschrift zur Barzahlung (sofern es eine solche gibt) an die Regelung des § 3 SächsEGovG anzupassen. Hierfür ist bei Bedarf die zuständige Rechtsaufsicht einzuschalten oder fachaufsichtlicher Rat einzuholen.

Für alle anderen gebührenpflichtigen Geschäftsfälle ist zu prüfen, inwieweit die existierenden Möglichkeiten einer unbaren Zahlung bereits eingesetzt werden (kein Handlungsbedarf) oder eingesetzt werden können (Handlungsbedarf). Für die Identifikation von Geschäftsfällen bei denen Handlungsbedarf besteht, wird folgendes Vorgehen vorgeschlagen.

B.1 Einordnung relevanter Geschäftsfälle anhand bereits vorliegender Unterlagen

Im jeweiligen Geschäftsbereich ist anhand vorliegender Unterlagen zu prüfen, ob gebührenpflichtige Geschäftsfälle vorkommen. Als Unterlagen kommen z. B. Gebührenordnungen, Satzungen und Bescheide in Frage. Das Prüfungsergebnis könnte wie folgt strukturiert sein.

1	*2*	*3*	*4*	*5*
Geschäftsfall (Kurz-bezeich-nung)	Enthalten ALLE Zahlungsauffor-derungen für diesen Geschäfts-fall den Hinweis auf die elektronische Zahlmöglichkeit? (ja / nein)	Kann die Behörde bei diesem Geschäftsfall – sofern der Verwaltungs-kunde den elektroni-schen Zahlungsweg wählt – die Zahlung, wenn notwendig, im Haushalt zuordnen? (ja / nein / nicht notwendig)	Ist die Zahlung bereits elektronisch, z. B. durch Überweisung auf ein Konto, möglich? (ja / nein)	optional: Anzahl / Volumen je Jahr
[…]				

<u>Hinweise zur Prüftabelle:</u>

Spalte 1: Die Spalte sollte eine eindeutige Bezeichnung enthalten, die in der gesamten Behörde gleich gut verstanden wird.
Spalte 2: Es sind hier nicht nur alle Formulare, Schreiben usw., die in Papierform an den Behördenkunden versandt werden, durchzusehen, sondern auch die in Online-Angeboten enthaltenen Zahlungsinformationen.
Spalte 3: Besonders wichtig ist hier, dass eine Zuordnung im Haushalt auch dann gegeben sein muss, wenn bisher üblicherweise eine Bareinzahlung an der Kasse erfolgte, künftig aber als zusätzlicher Weg auch eine Überweisung ermöglicht sein muss. Bei einem elektronischen Zahlungsvorgang muss stets ersichtlich sein, wofür eine Zahlung geleistet wird.
Spalte 4: Hier kann nur dann eindeutig »ja« eingetragen werden, wenn die Spalten 2 und 3 jeweils ein »ja« enthalten oder Spalte 2 mit »ja« und Spalte 3 mit Zuordnung »nicht notwendig« beantwortet werden kann.
Spalte 5: Diese optionale Spalte kann (auch mit Schätzwerten) ausgefüllt werden, wenn beabsichtigt ist, Geschäftsfälle zu identifizieren, für die sich möglicherweise ein medienbruchfreies Verfahren lohnen würde. Je höher die Anzahl ist, desto wahrscheinlicher ist der Nutzen, diesen Geschäftsfall elektronisch verfügbar zu machen.

Anhand dieser Prüftabelle kann leicht festgestellt werden, ob ein Handlungsbedarf vorliegt. Dieser Handlungsbedarf richtet sich ausschließlich auf die Realisierung des vom Gesetzgeber geforderten Minimums.

Für die Behörde und den Behördenkunden effektivere, einfachere oder bequemere Lösungen (z. B. zur Vermeidung von Medienbrüchen) werden im folgenden Abschnitt beschrieben.

B.2 Weitere Umsetzungsmöglichkeiten

Für eine »zeitgemäße« Umsetzung elektronischer Zahlungen hat der Gesetzgeber ebenfalls den Weg geebnet. § 3 SächsEGovG und die zugehörige Begründung erlauben auch den Einsatz der bereits etablierten Zahlungsverkehrs-Software (Produktname: ePayBL®, E-Payment-Bund-Länder) der E-Government-Plattform des Freistaates Sachsen (Basiskomponente Zahlungsverkehr, BaK ZV). Behörden, die (z. B. zur Effizienzsteigerung des Haushalts- und Kassenwesens oder für einen verstärkten Bürgerservices) über die gesetzliche Pflicht hinaus Online-Zahlverfahren anbieten möchten, können dies auf einfache Art und Weise tun.

Die derzeit über die BaK ZV verfügbaren Zahlverfahren (Vorkasse / auf Rechnung, Lastschrift (SEPA-Lastschrift), giropay® und Kreditkarte) decken die üblichen – auch im zivilrechtlichen Zahlungsverkehr verwendeten – Online-Zahlarten ab.

Dabei können vorhandene und bewährte Module genutzt werden, die gemeinsam mit dem Bedarfsträger (Behörde, Auftraggeber) für den jeweiligen Einsatzzweck passend ausgewählt und in Betrieb genommen werden. Vor der Einführung wird eine Beratung durch die Anwendungsbetreuung der BaK ZV, durch den Basiskomponenten-Verantwortlichen oder durch einen damit beauftragten Dritten empfohlen.

Für die Behörden im Freistaat Sachsen ist diese normale Nutzung der BaK ZV kostenfrei. Es fallen möglicherweise (je nach ausgewählter Zahlart) verbrauchsabhängige Kosten (vergleichbar mit Porto) an. Sofern nicht XFinanz als Standard-Schnittstelle genutzt wird, kommen Kosten für eine Integration in das jeweilige Fachverfahren / Haushaltssystem hinzu, falls eine Anbindung nötig ist oder gewünscht wird.

Als Module der BaK ZV stehen derzeit bereit:

- **Kernsystem** – wird immer benötigt
- **Paypage** – als einfache Integrationsmöglichkeit in das jeweilige Fachverfahren
- **Rechnungserstellung** – einfache Möglichkeit, um Einzel- oder Massenversand der über die Paypage bezahlbaren Rechnungen zu realisieren
- **Webshop** – einfache Möglichkeit, Verwaltungsdienstleistungen oder -produkte kostenpflichtig bereitzustellen. Es können beispielsweise auch Eintrittskarten für Veranstaltungen angeboten und gebucht werden. Eine Auswahl derzeit bereits produktiver Angebote der BaK ZV ist online auf der Webseite zu E-Shops in der öffentlichen Verwaltung zu finden.
- **Bezahl-Terminals** – Der Staatsbetrieb SID hat für den Freistaat Sachsen einen Rahmenvertrag abgeschlossen, der es allen öffentlichen Verwaltungen im Freistaat ermöglicht, durch den Abruf von Bezahlterminals den Einsatz elektronischer Kartenzahlungen zu ermöglichen. Der hierfür notwendige Abrufprozess ist weitgehend automatisiert.

B.3 Kontaktmöglichkeiten

Für Rückfragen steht die Betreuung der BaK ZV zur Verfügung.

Staatsbetrieb Sächsische Informatik Dienste
Fachbereich 3.1 | E-Government- und Querschnittverfahren
Betreuung BaK ZV
Riesaer Straße 7
01129 Dresden
Tel.: 0351 20545-178
E-Mail: zv@sid.sachsen.de

C Beantwortung häufig gestellter Fragen

Frage 1: Warum sollte ich die Basiskomponente Zahlungsverkehr (ePayBL®) einsetzen und nicht einfach ein kommerzielles Tool (z. B. PayPal®)?

Antwort: ePayBL® hat im Vergleich zu kommerziellen Tools folgende Vorteile:

1. Verwaltungskunden (Bürger, Unternehmen), die z. B. kein Konto bei PayPal® oder Click-and-Buy® haben, werden nicht ausgeschlossen.
2. Es muss kein eigener Vertrag mit einem Zahlungsverkehrsprovider verhandelt werden – ein bestehender Rahmenvertrag kann genutzt werden, sofern hierfür im Rahmen der Ausschreibung der Bedarf angezeigt wurde. Bitte erkundigen Sie sich, ob Sie zum Kreis der Abrufberechtigten gehören (zv@sid.sachsen.de).
3. Die Bereitstellung von Daten für das Haushaltssystem erfolgt automatisiert. Nacharbeiten werden daher auf ein Minimum reduziert.
4. Für kommerzielle Tools fallen meist höhere Kosten pro Buchung an.

Frage 2: Was muss ich tun, um mir einen Überblick über Details und weitere Dokumente von ePayBL® zu verschaffen?

Antwort: Jeder Interessent kann weitere Informationen formlos über die E-Mail-Adresse zv@sid.sachsen.de anfordern.

Frage 3: Welche Haushaltssysteme werden von ePayBL® bereits unterstützt?

Antwort: Derzeit werden verschiedene Haushaltssysteme in unterschiedlicher Tiefe unterstützt. Im staatlichen Bereich sind es SaxMBS und Agresso, im kommunalen Bereich wurden (teilweise nur kameral) die Systeme Infoma, SAP FI, CIP und Saskia umgesetzt. Weitere sollen folgen.

Frage 4: Wie hoch ist der Aufwand für den Einsatz von ePayBL®?

Antwort: Je nachdem, in welcher Tiefe und mit welchen Modulen eine Umsetzung erfolgen soll, variieren die Kosten sehr. Prinzipiell ist es möglich, eine Fachanwendung mit wenig Aufwand für die Vereinnahmung von Online-Zahlungen zu ertüchtigen. Voraussetzung hierfür ist eine genaue Kenntnis der Geschäftsprozesse (z. B.: Um welchen Verwaltungsvorgang handelt es sich? An welcher Stelle im Prozess soll die Zahlung erfolgen? Wohin sollen die Einnahmen im Haushalt fließen? Genügt vielleicht eine einfache Gutschrift auf das Konto? Wie erfolgt derzeit die Zuordnung von Zahlungseingängen zu den Zahlungspflichtigen?). Je einfacher der abzubildende

Prozess, desto geringer ist der Aufwand. Für die meisten der in den folgenden Beispielen genannten Aufgaben sind bei der Anwendungsbetreuung für die BaK ZV im Staatsbetrieb SID umfassende Erfahrungen vorhanden.

Beispiel 1: Die Buchung einer Teilnehmergebühr soll erfolgen.
Rahmenbedingungen:
- nur »sichere Zahlverfahren« (d. h. ohne Rückbuchungsmöglichkeit) sollen zum Einsatz kommen
- es genügt die Gutschrift auf dem Konto unter Angabe eines vom Fachverfahren vorgegebenen Verwendungszweckes zur Identifikation des Zahlungspflichtigen (keine Haushaltsanbindung)

Lösung:
- Integration der Paypage im Fachverfahren (dieses liefert Zahlbetrag, Zahlverfahren und Verwendungszweck)
- Zulassung von Kreditkarte und Giropay als Zahlverfahren

Aufwand:
- 1 Tag Schulung für den Programmierer der Fachanwendung
- ca. 10 h zur Einrichtung in der BaK ZV (inkl. Erstberatung)
- ca. 8 h Entwicklungs- und Testaufwand für Programmierer der Fachanwendung

Im praktischen Beispiel war so innerhalb einer halben Woche das System einsatzbereit.

Beispiel 2: Verwaltungsleistungen sollen über ein Shop-System angeboten werden.
Rahmenbedingungen:
- alle verfügbaren Zahlverfahren sollen zum Einsatz kommen
- die haushaltsrelevanten Daten sollen vom System bereitgestellt werden

Lösung:
- der von der BaK ZV bereitgestellte Webshop wird verwendet
- die im XFinanz-Format bereitgestellten Daten werden zur Buchung verwendet

Aufwand:
- ca. 1 Tag für das Aufsetzen des Webshops
- ca. 10 h zur Einrichtung in der BaK ZV (inkl. Erstberatung)
- interne Absprachen zwischen den Zuständigen (Haushalt, Recht, Organisation, IT-Fachverfahren, Öffentlichkeitsarbeit)
- Befüllung des Webshops mit Artikeln
- Anpassung des Webshop-Erscheinungsbildes an das eigene Corporate Design
- Anpassung von Impressum, AGB (sofern vorhanden)
- Ggf. Abschluss eines Vertrages zur ständigen Überprüfung auf Rechtssicherheit (Reduzierung Abmahnrisiko)

§ 5 Abs. 1 SächsEGovG – Datenschutz- und Informationssicherheitskonzepte

§ 5 Abs. 1 SächsEGovG lautet:

»Zur Gewährleistung des Datenschutzes erstellen und pflegen die staatlichen Behörden und die Träger der Selbstverwaltung, die personenbezogene Daten automatisiert verarbeiten, Datenschutz- und Informationssicherheitskonzepte.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung der Träger der Selbstverwaltung (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG), Datenschutz- und Informationssicherheitskonzepte für die elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit zu erstellen, wenn sie personenbezogene Daten automatisiert verarbeiten, gilt unmittelbar mit Inkrafttreten des Gesetzes seit dem 9. August 2014.

Inhalt der Verpflichtung

Aus dem verstärkten Einsatz informationstechnischer Systeme in der Verwaltung ergeben sich neben den Verbesserungen für die damit unterstützten Verwaltungsprozesse, auch gesteigerte Gefahrenlagen insbesondere für die in diesen Systemen verarbeiteten personenbezogenen Daten. Daher verpflichtet § 5 Abs. 1 SächsEGovG die staatlichen Behörden und die Träger der Selbstverwaltung zur Erstellung und Pflege individueller Datenschutz- und Informationssicherheitskonzepte, mit denen für die einzelnen in der sächsischen Verwaltung eingesetzten informationstechnischen Systeme die technisch-/organisatorische Gewährleistung eines rechtskonformen Datenschutzes abgesichert wird.

Nach § 5 SächsEGovG sind Datenschutz- und Informationssicherheitskonzepte nur zu erstellen, wenn dabei **personenbezogene Daten automatisiert verarbeitet** werden. Nach § 3 Abs. 5 SächsDSG liegt eine automatisierte Verarbeitung personenbezogener Daten dann vor, wenn diese durch Einsatz eines elektronischen Datenverarbeitungssystems programmgesteuert durchgeführt wird.

Der Fokus dieser Konzepte ist daher auf den Schutz der personenbezogenen Daten gerichtet. Dem gegenüber liegt der Fokus bei der Umsetzung der Regelungen in §§ 9 Abs. 2, 13 Abs. 1 SächsEGovG auf der Informationssicherheit der Daten als solcher. Nach § 3 Abs. 1 SächsDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Dies sind z. B. Name, Adresse, Eigenschaften einer Person, aber auch Beziehungen zur Umwelt oder Eigentumsverhältnisse. Im E-Government handelt es sich einerseits um die Daten von Bürgern, die bei der Kommunikation mit der Verwaltung und bei der Erledigung von Verwaltungsaufgaben anfallen und andererseits um die personenbezogenen Daten von Mitarbeitern, die z. B. als Protokolldaten im IT-Verfahren anfallen oder den so genannten Amtsträgerdaten wie Name und Funktionsbezeichnung, die von öffentlichen Stellen in ihren online- Angeboten veröffentlicht werden.

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

Unter einem **Datenschutzkonzept** versteht man ein Dokument, das Auskunft über die Rechtmäßigkeit der Datenverarbeitung bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gibt. Das Datenschutzkonzept gehört neben dem Fachkonzept, dem Betriebskonzept und dem Sicherheitskonzept zur Dokumentation von IT-Verfahren. Das Datenschutzkonzept dokumentiert für die datenschutzrechtliche Beurteilung notwendige Informationen zur Verarbeitung personenbezogener Daten, auch im Hinblick auf Art, Umfang, Tiefe und Ausmaß der Verarbeitung personenbezogener Daten. Mit diesem Konzept kann auch die Angemessenheit der getroffenen personellen, technischen und organisatorischen Maßnahmen zum Datenschutz betrachtet werden.

Für alle personenbezogenen Daten abhängig von ihrer Sensibilität oder einer besonderen Schutzwürdigkeit müssen die angemessenen personellen, technischen und organisatorischen Maßnahmen getroffen werden, die erforderlich sind, um eine den Vorschriften des Datenschutzgesetzes entsprechende Datenverarbeitung zu gewährleisten (§ 9 SächsDSG).

Daten, die dem Sozialgeheimnis oder einem anderen besonderen Amts- oder Berufsgeheimnis unterliegen, sind nach spezialgesetzlichen Regelungen besonders geschützt.

Bei der elektronischen Übermittlung der Daten unter Nutzung von E-Government-Anwendungen, z. B. der Inanspruchnahme von E-Mail-Diensten oder Online-Verbindungen des Bürgers zur Verwaltung, handelt es sich rechtlich um die Inanspruchnahme von Telekommunikations- und Tele- oder Mediendiensten. Entsprechende Regelungen finden sich im Telemediengesetz und im Telekommunikationsgesetz.

Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität sowie Verfügbarkeit von Informationen und IT durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen. Neben personenbezogenen Daten sind auch nicht personenbezogene Daten, z. B. Geschäfts- und Betriebsgeheimnisse angemessen zu schützen.

Informationssicherheitskonzepte beschreiben technische, personelle und organisatorische Maßnahmen, mit denen Informationen und IT gegen die verschiedenen Risiken geschützt werden können. In einem **Informationssicherheitskonzept** (IT-Sicherheitskonzept) werden im Unterschied zum Datenschutzkonzept auch Sicherheitsfragen zu nicht personenbezogenen Daten beschrieben. Grundlage für ein IT-Sicherheitskonzept ist im Regelfall eine Sicherheitsbetrachtung mit Risikoanalyse auf der Basis einer Bedrohungsanalyse.

Die für eine Behörde oder Einrichtung geltenden spezifischen Informationssicherheitsziele und -strategien als Grundlage für die Erstellung von Informationssicherheitskonzepten sind in einer Leitlinie zur Informationssicherheit festzuhalten. Für staatliche Behörden und Einrichtungen in Sachsen gelten dabei die Regelungen der VwV Informationssicherheit. Für Träger der kommunalen Selbstverwaltung liegt eine Musterleitlinie vor, die diese als Vorlage für die Erstellung einer eigenen Leitlinie verwenden können.

Über § 13 i. V. m. § 9 Abs. 2 SächsEGovG kann es jedoch ggf. erforderlich werden, das datenschutzbezogene Informationssicherheitskonzept auch auf andere nicht personenbezogene Datenschutzziele und sonstige IT-Sicherheitsbetrachtungen zu erweitern (siehe Empfehlungen zu § 13 i. V. m. § 9 Abs. 2 SächsEGovG in diesem Handlungsleitfaden).

Datenschutz- und Informationssicherheitskonzepte müssen daher in Kenntnis dieser Regelungen abgefasst sein und entsprechende Anforderungen berücksichtigen.

Die Konzepte dienen nicht nur zur Eigenkontrolle der datenverarbeitenden Stelle, sondern auch als Kontrollunterlage für den behördlichen und den Sächsischen Datenschutzbeauftragten sowie weitere Stellen, wie z. B. die Personalverwaltung oder die interne Revision. Nur bei Vorliegen der Konzepte kann die datenverarbeitende Stelle nachweisen, dass die vorgesehene Datenverarbeitung in Übereinstimmung mit den datenschutz- und informationssicherheitsrechtlichen Vorgaben umgesetzt wird.

Datenschutz und Informationssicherheit sind Daueraufgaben. Die Dynamik der Verfahren zur Verarbeitung personenbezogener Daten fordert eine ständige Sicherstellung des benötigten Datenschutz- und Informationssicherheitsniveaus. Deshalb sind während der Nutzung des Verfahrens bei Vorschriftenänderungen, technischen Änderungen, Erweiterung der Funktionalität etc. die Konzepte kontinuierlich fortzuschreiben.

Dieser Handlungsleitfaden enthält im Folgenden maßgebliche Aspekte für die Einhaltung des Datenschutzes und der Informationssicherheit im Rahmen von E-Government für die Erstellung von Datenschutz- und Informationssicherheitskonzepten sowie praktische Beispiele.

Im Übrigen sei auf die im Anhang zu diesem Handlungsleitfaden befindliche Checkliste zur Erstellung von Datenschutz- und Informationssicherheitskonzepten verwiesen, welche die nachfolgenden Erläuterungen zusammenfassend darstellt.

B Empfehlungen zur Umsetzung

B.1 Allgemeine übergreifende Festlegungen

B.1.1 Verantwortlichkeiten im Datenschutz festlegen

Die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung trägt die Verwaltung, welche die Daten zur Erfüllung ihrer Aufgaben verarbeitet. Bei der elektronisch unterstützen öffentlich-rechtlichen Verwaltungstätigkeit erfordert dies die Schaffung geeigneter Organisationsstrukturen sowie klare Festlegungen, wer für welche Aufgaben verantwortlich ist und wer die Verantwortung für die Vollständigkeit und Korrektheit von Daten und Verfahren trägt. Dies ist im Konzept schriftlich zu dokumentieren, auch die Verfahrensweise der Beteiligung des behördlichen Datenschutzbeauftragten und des Sächsischen Datenschutzbeauftragten sollte festgelegt werden.

Alle verfahrensmäßigen und technisch-organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit müssen konsequent umgesetzt und in ihren Wirkungen im Rahmen eines begleitenden Controllings beobachtet werden. Nur so ist sichergestellt, dass die Effektivität der Maßnahmen gewährleistet bleibt, Fehlentwicklungen oder Vollzugsdefizite frühzeitig entdeckt und notwendige Weiterentwicklungen zeitgerecht eingeleitet werden können. Die Überwachung der Einhaltung von Datenschutzvorgaben ist Aufgabe der jeweils verantwortlichen Führungskräfte und der behördlichen Datenschutzbeauftragten.

Zur Bestellung von behördlichen Datenschutzbeauftragten siehe § 11 SächsDSG. Weitere Informationen sowie Formblätter finden sich in der Bekanntmachung des SächsDSB zur Bestellung von Datenschutzbeauftragten öffentlicher Stellen vom 11. März 2004.

Eine Musterdienstanweisung über die Organisation des Informations- und Datenschutzes findet sich auf der Website des Sächsischen Datenschutzbeauftragten.

Zur Regelung der Verantwortlichkeiten siehe auch BSI-Maßnahmenkataloge M 2.502 Regelung der Verantwortlichkeiten im Bereich Datenschutz.

B.1.2 Verpflichtung der Mitarbeiter auf das Datengeheimnis

Gemäß § 6 Abs. 2 SächsDSG sind Bedienstete bei der Aufnahme ihrer Tätigkeit über die Wahrung des Datengeheimnisses zu unterrichten und auf dessen Einhaltung zu verpflichten. Weitere Informationen enthält das Merkblatt des Sächsischen Datenschutzbeauftragten zur Verpflichtung auf das Datengeheimnis.

Auf der Website des Sächsischen Datenschutzbeauftragten sind außerdem die entsprechenden Formblätter für die Verpflichtung zu finden.

B.2 Verfahrensverzeichnis und Vorabkontrolle

B.2.1 Verfahrensverzeichnis nach § 10 SächsDSG

Nach § 10 Abs. 1 S. 1 SächsDSG hat jede Daten verarbeitende Stelle ein **Verzeichnis über die bei ihr eingesetzten automatisierten Verarbeitungsverfahren** zu führen.

Nähere Erläuterungen und ein Formular zur Erfassung der Daten enthält die Bekanntmachung des Sächsischen Datenschutzbeauftragten zum Verzeichnis automatisierter Verarbeitungsverfahren vom 11. März 2004.

B.2.2 Vorabkontrolle – § 10 Abs. 4 SächsDSG

Die datenschutzrechtliche Vorabkontrolle erfolgt vor dem erstmaligen Einsatz oder der wesentlichen Änderung

- eines automatisierten Abrufverfahrens (§ 8 SächsDSG),
- eines automatisierten Verfahrens, in dem besonders schutzwürdige Daten (z. B. Gesundheitsdaten) verarbeitet werden (§ 4 Abs. 2 SächsDSG) oder
- eines automatisierten Verfahrens, in dem Daten von Beschäftigten (§ 37 SächsDSG) verarbeitet werden. Dabei sind Beschäftigtendaten sehr weit zu verstehen und umfassen nicht nur Personalaktendaten, sondern z. B. auch Daten zur Internetnutzung.

Gemäß § 10 Abs. 4 SächsDSG ist grundsätzlich vor der Einführung einer solchen E-Government-Anwendung zu prüfen, ob die Datenverarbeitung zulässig ist und die vorgesehenen personellen, technischen und organisatorischen Maßnahmen nach § 9 SächsDSG ausreichend sind. Die Vorabkontrolle umfasst eine Prüfung der Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der Datenverarbeitung, die schriftlich zu dokumentieren ist.

Ist die Verarbeitung der personenbezogenen Daten rechtmäßig, stellt die Vorabkontrolle für die einzuführenden automatisierten Verfahren den Schutzbedarf und die Risiken fest und bewertet, insbesondere unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 9 SächsDSG, ob und wie Gefahren für die informationelle Selbstbestimmung Betroffener angemessen verhindert werden können.

Ist für die öffentliche Stelle (i. S. v. § 2 Abs. 1 und 2 SächsDSG), bei der ein E-Government-Verfahren eingesetzt oder wesentlich geändert werden soll, ein behördlicher Datenschutzbeauftragter (i. S. v. § 11 SächsDSG) bestellt, so führt dieser die Vorabkontrolle durch, andernfalls der Sächsische Datenschutzbeauftragte. Die Anzeigepflicht für ein solches

Verfahren obliegt der Daten verarbeitenden Stelle. Sie hat dafür die zur Prüfung erforderlichen Unterlagen frühestmöglich zur Verfügung zu stellen.

Nähere Erläuterungen sowie ein Formular zur Erfassung der Daten enthält die Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Vorabkontrolle § 10 Abs. 4 SächsDSG vom 12. September 2005 in der aktualisierten Fassung vom 1. Februar 2007.

In den folgenden Abschnitten werden die zur Erstellung eines Datenschutzkonzeptes, zur Führung des Verfahrensverzeichnisses und zur Durchführung einer Vorabkontrolle erforderlichen technischen und organisatorischen Festlegungen dargestellt und erläutert.

B.3 Bestandteile von Datenschutz- und Informationssicherheitskonzepten

B.3.1 Ziel des Einsatzes und rechtlicher Rahmen des eingesetzten Verfahrens

Die Verarbeitung personenbezogener Daten stellt nach der Rechtsprechung des Bundesverfassungsgerichts einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, der einer ausdrücklichen gesetzlichen Erlaubnis oder einer Einwilligung des Betroffenen bedarf. Zu den Rechtsvorschriften, aus denen sich eine Erlaubnis für eine Datenverarbeitung ergeben kann, zählen neben allgemeinen Datenschutzgesetzen (z. B. SächsDSG) und Spezialgesetzen auch Rechtsverordnungen und Satzungen, die von einer juristischen Person des öffentlichen Rechts im Rahmen der ihr verliehenen Autonomie erlassen werden, sowie allgemein verbindliche tarifvertragliche Regelungen und Dienstvereinbarungen zwischen Dienststelle und Personalvertretung.

Fehlt eine einschlägige Rechtsvorschrift, darf die Datenverarbeitung im Rahmen der Erfüllung der gesetzlich übertragenen Aufgaben durch die Behörde nur mit vorheriger Zustimmung des Betroffenen erfolgen (Einwilligung). Die Anforderungen an eine Einwilligung sind in § 4 Abs. 3 bis 5 SächsDSG genau vorgegeben. Die Einwilligung bedarf grundsätzlich der Schriftform. Sie muss den Betroffenen »informieren«, das heißt, sie muss den Zweck der Datenverarbeitung, die Empfänger einer vorgesehenen Datenübermittlung sowie das Recht zur Verweigerung der Einwilligung und die etwaigen Folgen der Verweigerung enthalten (§ 4 Abs. 2 S. 1 SächsDSG). Rechtsnachteile dürfen dem Betroffenen durch die Verweigerung der Einwilligung nicht entstehen (§ 4 Abs. 2 S. 2 SächsDSG).

B.3.2 Festlegung der zu verarbeitenden personenbezogenen Daten

Die zu verarbeitenden personenbezogenen Daten (Bürger- und Mitarbeiterdaten) können entweder direkt im Gesetz aufgeführt sein, wie z. B. in § 5 SächsMG, oder sie sind nach ihrer Erforderlichkeit für die Erfüllung der gesetzlichen Aufgaben zu bestimmen.

Erforderlichkeit für die Aufgabenerfüllung

Eine Verarbeitung personenbezogener Daten ist nur erforderlich, wenn die jeweilige Aufgabe ohne das konkrete Datum nicht oder nicht vollständig erfüllt werden kann. Dazu zählt auch, dass die Aufgabe auf andere Weise nur unter unverhältnismäßig großen Schwierigkeiten, mit einem unvertretbar höheren Aufwand oder verspätet erfüllt werden könnte. Eine Datenerhebung »auf Vorrat« ist unzulässig.

Beispiele für die Prüfung der Erforderlichkeit:

- Bei E-Mail-Newslettern reicht z. B. die Erhebung der E-Mail-Adresse der Empfänger aus; die Erfassung des Namens und der postalischen Anschrift hat zu unterbleiben.

- Bei Angeboten im Internet ist auf eine vollständige Erfassung der IP-Adressen der Nutzer zu verzichten, da diese für die Erbringung des Angebots und seine Abrechnung nicht erforderlich ist und gegen § 15 Abs. 1 Telemediengesetz verstößt. Für die statistische Auswertung reichen gekürzte IP-Adressen aus.
- Elektronische Erhebungsformulare sind so zu gestalten, dass im Regelfall nur diejenigen Daten abgefragt werden, die für die jeweilige Aufgabe erforderlich sind. Sofern auch »Überschussdaten« erhoben werden, ist ausdrücklich auf die Freiwilligkeit der entsprechenden Angaben hinzuweisen. Bei der Übernahme analoger Formulare im Rahmen von E-Government-Anwendungen ist vorab besonders kritisch zu prüfen, ob wirklich alle bisher erhobenen Daten für die Aufgabenerledigung der Verwaltung erforderlich sind.

Prüfung der Geeignetheit

Die Erforderlichkeit setzt die Geeignetheit voraus, das heißt Daten, die zur Erreichung des Verarbeitungszieles überhaupt nicht geeignet sind, sind schon von daher auch nicht erforderlich. Ggf. ist von der Möglichkeit der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Die Einhaltung des Erforderlichkeitsgrundsatzes im Einzelfall ist bereits in der Konzeptions- und Planungsphase von E-Government-Anwendungen und bei der Systemauswahl zu berücksichtigen. Das Gebot der Erforderlichkeit gilt für alle Phasen der Verarbeitung, nicht nur für die Erhebung, sondern auch für den gesamten anschließenden Verarbeitungsprozess.

Grundsatz der Zweckbindung

Da bei E-Government-Anwendungen verknüpfbare Sammlungen von personenbezogenen Daten entstehen, muss besonders darauf geachtet werden, dass diese Daten wirklich nur für die Zwecke verwendet werden, für die sie erhoben und gespeichert wurden. Der Zweck der Datenverarbeitung folgt aus der jeweiligen Fachaufgabe, zu deren Erfüllung die Daten erhoben wurden. Sofern Daten der öffentlichen Stelle ohne Erhebung zur Kenntnis gelangt sind, legt sie den Zweck bei der erstmaligen Speicherung fest. Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck ist als Zweckänderung oder Zweckdurchbrechung nur auf gesetzlicher Grundlage (z. B. § 13 Abs. 2 SächsDSG) oder dann zulässig, wenn der Betroffene eingewilligt hat. Eine verstärkte Zweckbindung besteht für Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Ein striktes Verbot der Zweckänderung besteht für Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

Dies gilt auch dann, wenn die Daten innerhalb der Behörde an eine andere Stelle mit einer anderen, über bloße Hilfsfunktionen hinausgehenden Aufgabenstellung weitergegeben werden sollen; denn die öffentliche Verwaltung stellt keine Informationseinheit dar, es gilt der Grundsatz der informationellen Gewaltenteilung. Vor der Übermittlung der Daten ist daher die Zulässigkeit zu prüfen.

Grundsätze der Datenvermeidung und Datensparsamkeit

Die Grundsätze der Datenvermeidung und Datensparsamkeit gemäß § 9 Abs. 1 S. 2 SächsDSG fordern es, schon im Vorfeld bei der Entwicklung und Auswahl von Datenverarbeitungssystemen und bei der Ausgestaltung der konkreten Datenverarbeitungsprozesse darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden. Damit wird ein allgemeines Gestaltungsprinzip vorgegeben, das das Entstehen von

Daten mit Personenbezug oder Personenbeziehbarkeit von vornherein ausschließen oder auf ein Minimum beschränken will.

B.3.3 Ermittlung des Schutzbedarfes der verarbeiteten Daten

Der Schutzbedarf der zu verarbeitenden Daten ist pro Schutzziel gemäß § 9 Abs. 2 SächsDSG festzulegen. Er ist pauschal umso höher anzusetzen, je größer der potentielle Schaden ist und je später der Schaden bemerkt werden kann. Die gesetzlich geregelten datenschutzrechtlichen Schutzziele sind Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Transparenz und Revisionsfähigkeit.

Personenbezogene Daten sind im Hinblick auf den Schutzbedarf sowohl einzeln als auch im Gesamtkontext der Anwendung zu bewerten. Wirken verschiedene Stellen an der E-Government-Anwendung mit, ist darauf zu achten, dass die Daten der beteiligten Einrichtungen insgesamt bewertet werden.

Die Ausgestaltung der Schutzmaßnahmen muss sich daran orientieren, welche Folgen für einen Betroffenen durch die Beeinträchtigung des informationellen Selbstbestimmungsrechts entstehen können (Betroffenensicht) und welcher potentielle Schaden für den Betreiber (Betreibersicht) eintreten kann. Jede Behörde und Einrichtung muss dabei im Rahmen ihrer Eigenverantwortung für den Datenschutz und die Informationssicherheit den Schutzbedarf der von ihr verarbeiteten Daten selbst einschätzen. Als Grundlage kann die vom BSI vorgeschlagene und im Folgenden überblicksmäßig wiedergegebene Einteilung in die Schutzbedarfskategorien »NORMAL«, »HOCH« und »SEHR HOCH« dienen.

Anhaltspunkte für einen **Schutzbedarf »NORMAL«** könnten z. B. sein, wenn

- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts durch den Einzelnen noch als geringfügig eingeschätzt würde;
- ein möglicher Missbrauch personenbezogener Daten nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen hätte;
- eine Beeinträchtigung der persönlichen Unversehrtheit nicht möglich erscheint;
- für den Betreiber der Anwendung nur eine geringe Ansehens- oder Vertrauensbeeinträchtigung zu erwarten wäre.

Anhaltspunkte für einen **Schutzbedarf »HOCH«** könnten z. B. sein, wenn

- eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen möglich erscheint;
- ein möglicher Missbrauch personenbezogener Daten erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen hätte;
- eine Beeinträchtigung der persönlichen Unversehrtheit nicht absolut ausgeschlossen werden kann;
- für den Betreiber der Anwendung eine breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten wäre.

Anhaltspunkte für einen **Schutzbedarf »SEHR HOCH«** könnten z. B. sein, wenn

- eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen möglich erscheint;
- ein möglicher Missbrauch personenbezogener Daten für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten würde;
- gravierende Beeinträchtigungen der persönlichen Unversehrtheit oder Gefahr für Leib und Leben möglich ist;
- für den Betreiber der Anwendung eine landes- oder bundesweite Ansehens- oder Vertrauensbeeinträchtigung denkbar ist.

Als Hilfsmittel zur Orientierung können die Hinweise zur Schutzbedarfsfeststellung im BSI-Standard 100-2 (vor allem Kapitel 4.3 – Schutzbedarfsfeststellung) angewendet werden (Hinweise zur Schutzbedarfsfeststellung im BSI-Standard 100-2).

B.3.4 Aufzählung und Beschreibung der eingesetzten IT-Komponenten

Vor der Inbetriebnahme des Verfahrens ist zu prüfen, ob die Datenverarbeitung zulässig ist und die vorgesehenen personellen, technischen und organisatorischen Maßnahmen nach z. B. § 9 SächsDSG ausreichend sind, um eine den datenschutzrechtlichen Vorschriften entsprechende Datenverarbeitung zu gewährleisten. Dazu müssen die technischen Komponenten und deren technisches Zusammenwirken so beschrieben und festgelegt sein, dass auf dieser Grundlage eine Bewertung erfolgen kann, ob beim Einsatz die Risiken für das informationelle Selbstbestimmungsrecht ausreichend vermieden werden.

B.3.5 Prozessbezogene Verfahrensbeschreibung

In den Verfahrensbeschreibungen soll die Verfahrensweise bei der Verarbeitung personenbezogener Daten vollständig und aktuell dokumentiert werden. Im Sinne eines angepassten Benutzerhandbuchs werden alle genutzten Bedienmöglichkeiten und Funktionalitäten des eingesetzten Verfahrens beschrieben.

B.3.6 Dokumentation der Festlegung der erforderlichen technischen und organisatorischen Maßnahmen

Das Recht auf informationelle Selbstbestimmung verlangt neben dem rechtlichen Schutz der personenbezogenen Daten eine angemessene Datensicherheit. Die Sicherungsziele sind von der Technologie unabhängig. Für jede E-Government-Anwendung sind die folgenden Gestaltungsanforderungen im Rahmen des Sicherheitskonzeptes konkret auszufüllen. Orientieren sollten sich die Maßnahmen an den Anforderungen der IT-Grundschutzkataloge des BSI. Laut VwV Informationssicherheit und § 9 Abs. 2 S. 3 SächsEGovG sind die Standards und Kataloge des BSI in der jeweils aktuellen Fassung für staatliche Behörden und Einrichtungen maßgeblich. Den Trägern der Selbstverwaltung wird die Anwendung von BSI-Grundschutz empfohlen. Angemessen sind die getroffenen Maßnahmen, wenn die Datenverarbeitungsvorgänge entsprechend des Schutzbedarfes der zu verarbeitenden Daten und einem eventuellen Gefährdungspotenzial gesichert sind. Die Maßnahmen müssen dem jeweiligen Stand der Technik entsprechen.

Die im Ergebnis notwendigen organisatorischen und technischen Maßnahmen zur Gewährleistung des informationellen Selbstbestimmungsrechts des Einzelnen sind festzulegen, zu

dokumentieren und konsequent umzusetzen. Ist deren Umsetzung nicht oder nur teilweise möglich, muss unter Umständen auf die weitere Realisierung des Vorhabens verzichtet werden.

Schutzziele und Maßnahmen zu deren Gewährleistung

Die **Vertraulichkeit** stellt sicher, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können.

Daran fehlt es z. B. beim Versand unverschlüsselter E-Mails. Die Übermittlung von Daten im Internet ohne technische Schutzvorkehrungen ähnelt einer mit Bleistift in Druckbuchstaben geschriebenen Postkarte. Der Inhalt kann von Dritten eingesehen und ohne Kenntnis des Absenders oder Adressaten verändert werden. In der analogen Papierwelt sind Änderungen in aller Regel nachvollziehbar – in der elektronischen Welt ist es dagegen ohne geeignete Gegenmaßnahmen möglich, die elektronischen Inhalte einzusehen und unbemerkt zu verändern.

Die **Integrität** gewährleistet, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

Verfügbarkeit für E-Government-Anwendungen ist gewährleistet, wenn die personenbezogenen Daten zeitgerecht und ordnungsgemäß verarbeitet werden können. Kritisch wird es, wenn Daten verloren gehen oder technische Defekte Rechner und Daten beeinträchtigen.

Authentizität: Personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können. Dabei ist zu unterscheiden zwischen dem Identitätsnachweis (die Kommunikationspartner weisen sich zweifelsfrei aus) und dem Herkunftsnachweis (der Absender weist nach, dass eine Nachricht von ihm stammt und nicht verändert wurde). Mit der Authentisierung sollen unberechtigte Zugriffe erkannt und abgewehrt werden sowie sensible Daten bei der Übertragung über Netze geschützt bleiben. Dazu sind Verfahren erforderlich, die allen Beteiligten die Feststellung der Identität ihrer Kommunikationspartner unmissverständlich ermöglichen.

Revisionsfähigkeit: Verantwortliche Stellen sind auch bei E-Government-Anwendungen verpflichtet, technische und organisatorische Maßnahmen zu treffen, damit nachträglich überprüft und festgestellt werden kann, wer welche personenbezogenen Daten zu welcher Zeit eingegeben und übermittelt hat. Auch Versuche missbräuchlicher Verarbeitung müssen nachträglich untersucht werden können. Mit einer Protokollierung wird einer missbräuchlichen Verwendung personenbezogener Daten vorgebeugt, weil keiner darauf vertrauen kann, dass Verstöße unentdeckt bleiben. Mit der Protokollierung entstehen allerdings besondere Sammlungen personenbezogener Daten über Nutzer. Daraus lassen sich Nutzerprofile ableiten oder Listen über Auffälligkeiten erstellen. Das Datenschutzrecht lässt das jedoch ohne Einwilligung der Betroffenen grundsätzlich nicht zu. Protokolldaten dürfen nur zu Zwecken genutzt werden, die Anlass für ihre Speicherung waren, und dürfen nicht für andere Zwecke verarbeitet werden. Im Einzelfall ist eine Auswertung der Protokolldaten zur Aufdeckung von Missbräuchen zulässig. Die Zweckbindung der Protokollierung muss daher technisch und organisatorisch sichergestellt werden. Der Grundkonflikt, der sich bei jeder Protokollierung mit dem Prinzip der Datenvermeidung und Datensparsamkeit ergibt, kann nur im Einzelfall gelöst werden.

Transparenz wird über die detaillierte Dokumentation der Verfahren erreicht, aus der sich ergibt, welche Daten wie verarbeitet werden, wie die Rechte Betroffener gewahrt werden und wie diese ihre Rechte selbst wahrnehmen können.

Das informationelle Selbstbestimmungsrecht für Betroffene setzt Kenntnis über die Struktur der Datenverarbeitung, über die Datenverarbeitungsprozesse, über die eingesetzte Technik und über die Datenströme voraus.

Die Rechte der Betroffenen (Verfahrensweisen, die die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung sicherstellen (§§ 18-23 SächsDSG))

Jede E-Government-Anwendung muss die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten und über die datenverarbeitenden Stellen informieren. Nur wenn die Betroffenen erfahren, welche personenbezogenen Daten über sie für welche Zwecke erhoben werden, wie die Struktur der Datenverarbeitung aussieht, wie die Datenverarbeitungsprozesse ablaufen und wer dafür die Verantwortung trägt, haben sie auch die Möglichkeit, ihre individuellen Rechte wahrzunehmen.

Zu den Rechten der Betroffenen gehören:

- Auskunft über die zu seiner Person gespeicherten Daten
- Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten
- Widerspruch gegen die Verarbeitung seiner Daten
- Schadensersatz
- Anrufung des zuständigen Landesdatenschutzbeauftragten
- Auskunft bei automatisierten Einzelentscheidungen

Bei der Nutzung gemeinsamer Verfahren ist die Regelung des § 6 Abs. 6 SächsEGovG zu beachten.

Weitere Informationen finden sich im Baustein B 1.5 Datenschutz auf der BSI-Website.

B.3.7 Weitere Festlegungen

Rollen und Zugriffsrechte festlegen

Einige technisch organisatorische Maßnahmen dienen der Sicherstellung mehrerer Schutzziele. Dazu gehört die Festlegung der Rollen und Zugriffsrechte. Die Festlegungen betreffen die Schutzziele Transparenz, Vertraulichkeit, Authentizität und Revisionsfähigkeit.

In E-Government-Projekten ist ein Rollen- und Zugriffsrechtekonzept zu erstellen, das regelt, welche Personen im Rahmen ihrer jeweiligen Funktion (Anwendungsentwickler, Systemadministrator, Anwenderbetreuer, Sachbearbeiter, Revisor, behördlicher Datenschutzbeauftragter) welche IT-Anwendungen und welche Daten nutzen dürfen. Dabei dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Alle am E-Government-Projekt beteiligten Personen sind vor der Aufnahme des Wirkbetriebes im erforderlichen Umfang zu schulen. In größeren Behörden kann es sinnvoll sein, eine zentrale Stelle (User-Help-Desk) mit der Betreuung der IT-Benutzer zu beauftragen und diese allen Mitarbeitern bekannt zu geben. Diese Maßnahme kann sich insbesondere im Hinblick auf die Unterstützung der Bürger, die mit der Verwaltung kommunizieren, als sinnvoll und praktikabel erweisen.

Für wichtige Teile der E-Government-Plattform liegt ein Rollenkonzept vor, das im Anhang zu diesem Handlungsleitfaden enthalten ist und als Beispiel verwendet werden kann.

Festlegungen zur Löschung von Daten

Nach § 20 Abs. 1 und 2 SächsDSG sind personenbezogene Daten zu löschen, wenn deren Speicherung unzulässig ist oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist und die Löschung nicht aus den in § 20 Abs. 3 und 4 SächsDSG aufgeführten Gründen zu unterbleiben hat.

Dabei bedeutet Löschen das Unkenntlichmachen von Daten, so dass sie für niemanden mehr zugänglich sind. Die Löschung hat unverzüglich, d. h. ohne schuldhaftes Zögern, zu erfolgen. Hinzuweisen ist jedoch auf die vorrangige Anbietungspflicht gemäß § 5 SächsArchivG. Wenn Aufbewahrungspflichten bestehen oder wenn anzunehmen ist, dass schutzwürdige Interessen des Betroffenen durch die Löschung beeinträchtigt werden, tritt an die Stelle der Löschung eine Sperrung.

Soweit sich solche nicht aus dem Gesetz ergeben (z. B. § 43 Abs. 1a SächsPolG), sind sie ggf. durch die verarbeitende Stelle unter Beachtung der gesetzlichen Aufbewahrungsfristen festzulegen (so auch ausdrücklich z. B. § 43 Abs. 4 SächsPolG). Um eine rechtskonforme, geordnete Löschung von personenbezogenen Daten sicherzustellen, sollten öffentliche Stellen daher entsprechende Festlegungen zur Löschung treffen und Verantwortlichkeiten zuweisen.

Die Löschung kann von modernen DV-Systemen dynamisch durchgeführt werden, d. h. bei Überschreiten eines bestimmten Termins (Löschfrist, Antragsende, Ablauf, der geforderte Nachweis wird erbracht) werden entsprechende Datenfelder gelöscht.

Weitere Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes finden sich in der Orientierungshilfe »Sicheres Löschen magnetischer Datenträger« vom Arbeitskreis »Technische und organisatorische Datenschutzfragen« der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Festlegungen zur Protokollierung

Ein wesentlicher Faktor der Systemsicherheit ist eine konsequente Revision. Hierbei sind die in Protokollen gesammelten Daten durch entsprechend autorisierte Mitarbeiter auszuwerten. Unregelmäßigkeiten beim Betrieb der IT-Systeme oder systematische Angriffe auf den Internet-Rechner und seine Komponenten können so aufgedeckt werden.

Revision beschränkt sich jedoch nicht auf die Kontrolle der Datenverarbeitungsvorgänge des eigenen IT-Systems. Werden Dienstleister mit der Verarbeitung personenbezogener Daten beauftragt, muss sich die Revision durch die Behörde auch auf deren IT-Systeme beziehen. Dabei ist insbesondere die Einhaltung der vertraglichen Regelungen zu prüfen.

Personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden, § 13 Abs. 4 SächsDSG.

Weitere Informationen finden sich in der Orientierungshilfe »Protokollierung« vom Arbeitskreis »Technische und organisatorische Datenschutzfragen« der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Festlegungen zur Auftragsdatenverarbeitung gemäß § 7 SächsDSG

Immer häufiger übertragen Verwaltungen einzelne Arbeitsabläufe oder ganze Aufgaben auf andere Stellen (Outsourcing). Dies wirft die Frage auf, wie dieser Vorgang datenschutz-

rechtlich zu bewerten ist, insbesondere welche Voraussetzungen für eine rechtmäßige Übertragung vorliegen müssen und ob es Grenzen für eine derartige Übertragung gibt.

Das Datenschutzrecht unterscheidet hierzu zwischen Datenverarbeitung im Auftrag und der Funktionsübertragung. Bei der Auftragsdatenverarbeitung liegt die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der personenbezogenen Daten beim Auftraggeber, der »Herr« seiner Daten bleibt. Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragnehmer vor. Dem Auftragnehmer wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter materieller Verantwortung des Auftraggebers, gewissermaßen als sein verlängerter Arm, übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine »Hilfsfunktion« der eigentlichen Aufgabe ausgelagert, ohne dass der Auftragnehmer einen eigenen Handlungs- oder Entscheidungsspielraum hat.

Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Auftragnehmer über die technische Durchführung hinaus materielle Leistungen mit Hilfe der überlassenen Daten oder bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Aufgabe, liegt eine Funktionsübertragung vor. In diesem Fall wird der Auftragnehmer zur Daten verarbeitenden Stelle und hat eigenständig für die zur Datensicherung und zur Gewährleistung von Vertraulichkeit erforderlichen technischen und organisatorischen Maßnahmen zu sorgen.

Die Bewertung, ob eine Auftragsdatenverarbeitung oder Funktionsübertragung vorliegt, lässt sich nur im Einzelfall vornehmen. Deutliche Erkennungsmerkmale bei Auftragsdatenverarbeitung sind die fehlende Entscheidungsbefugnis des Auftragnehmers, die weisungsgebundene Unterstützungstätigkeit und die fehlende Beziehung des Auftragnehmers zum Betroffenen. Merkmale der Funktionsübertragung sind die Überlassung von Nutzungsrechten an den Daten, die eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dritten sowie das Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch).

Besondere Probleme ergeben sich bei Daten, für die besondere Schutzvorschriften bestehen. Durch die Datenweitergabe werden die Daten dem Auftragnehmer offenbart. Dies ist unzulässig, wenn der Offenbarung gesetzliche Schutzvorschriften entgegenstehen. Dazu gehören insbesondere Berufsgeheimnisse (z. B. das Arztgeheimnis) und besondere Amtsgeheimnisse (wie das Steuergeheimnis). In diesen Fällen ist eine Weitergabe der Daten an Auftragnehmer nur zulässig, wenn die betreffenden Schutzvorschriften die Offenbarung dieser Daten erlauben.

Beauftragt eine öffentliche Stelle ein privates Dienstleistungsunternehmen oder einen anderen Auftragnehmer, um für sie Hardware, Software oder auch Tele- und Mediendienste zu betreiben und zu warten (Outsourcing), so ist dabei auf folgende Punkte zu achten:

- Der Auftragnehmer sollte kein eigenes, fachlich bestimmtes Interesse an einem Zugriff auf Inhaltsdaten haben (Eingrenzung der Gefahr eines Datenmissbrauchs).
- Bereits bei der Auswahl des Auftragnehmers ist darauf zu achten, dass er die erforderlichen technischen und organisatorischen Maßnahmen ergreifen kann. Das setzt voraus, dass alle wesentlichen Anforderungen bekannt sein müssen und sich der Auftraggeber davon überzeugt hat, dass der Auftragnehmer in der Lage ist, diese umzusetzen, bevor der Auftragnehmer erstmals Gelegenheit erhält, auf personenbezogene Echtdaten zuzugreifen.

Ein Mustervertrag zur Auftragsdatenverarbeitung gemäß § 7 SächsDSG findet sich auch auf der Website des Sächsischen Datenschutzbeauftragten.

C Beantwortung häufig gestellter Fragen

Frage 1: Wann sollten der zuständige Datenschutzbeauftragte und der Informationssicherheitsbeauftragte in ein E-Government-Projekt einbezogenen werden?

> **Antwort**: Sinnvoll ist die Beteiligung ab Projektinitialisierung, also frühestmöglich. Nur so können die rechtlichen Vorgaben zur Einhaltung des Datenschutzes und der Informationssicherheit eingehalten und ggf. Fehlinvestitionen vermieden werden, § 11 Abs. 4 Nr. 1 SächsDSG.

Frage 2: Muss der behördliche Datenschutzbeauftragte das Datenschutzkonzept selbst erstellen?

> **Antwort**: Der behördliche Datenschutzbeauftragte muss das Datenschutzkonzept nicht selbst erstellen. Die Zuständigkeit für die Erstellung des Datenschutzkonzeptes liegt gemäß § 5 Abs. 1 SächsEGovG bei den staatlichen Behörden und den Trägern der Selbstverwaltung. Ebenso wie bei Stellen, die keinen behördlichen Datenschutzbeauftragten bestellt haben, hat die Erstellung des Datenschutzkonzeptes vorrangig durch die Fachabteilung sowie die technischen Sachverständigen der Behörde zu erfolgen. Anhand derer kann der Datenschutzbeauftragte die Zulässigkeit des Einsatzes des Verfahrens feststellen und die technischen und organisatorischen Einsatzbedingungen insoweit bewerten, ob beim Einsatz Risiken für das informationelle Selbstbestimmungsrecht ausreichend vermieden werden. Sollte während der Erstellung Beratungsbedarf entstehen, kann sich der behördliche Datenschutzbeauftragte an den Sächsischen Datenschutzbeauftragten wenden. Gemäß § 10 Abs. 4 S. 6 SächsDSG hat der behördliche Datenschutzbeauftragte einer mit der Aufsicht betrauten Stelle das Ergebnis der Vorabkontrolle, wozu auch das Datenschutzkonzept gehört, nachgeordneten Stellen mitzuteilen. Ggf. ist externer Sachverstand einzukaufen.

Frage 3: Müssen ein Informationssicherheitskonzept und daneben ein Datenschutzkonzept erstellt werden?

> **Antwort**: Informationssicherheit und Datenschutz haben jeweils unterschiedliche Zielfunktionen. Bei der Informationssicherheit geht es um den Schutz der datenverarbeitenden Organisation und deren in Informationssystemen gespeicherten Daten durch geeignete Maßnahmen hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität. Beim Datenschutz geht es primär um die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung der von einer Informationsverarbeitung betroffenen Person. In dieses Grundrecht wird zulässigerweise eingegriffen, wenn öffentlichen Stellen auf gesetzlicher Grundlage die Verarbeitung personenbezogener Daten erlaubt ist. In der Folge müssen öffentliche Stellen daher darlegen, wie sie dieses Grundrecht ermöglichen und mögliche negative Auswirkungen auf dieses Grundrecht wirksam unterbinden. Viele Maßnahmen der Informationssicherheit und des Datenschutzes sind deckungsgleich. Aufgrund der unterschiedlichen Ziele sind aber auch Abwägungen vorzunehmen und Maßnahmen speziell für den Datenschutz zu treffen. Datenschutz

und Informationssicherheit können in einem Konzept betrachtet werden, wenn sich darin die vorab genannten Ziele in der gebotenen Klarheit nachvollziehen lassen.

Frage 4: Zu welchen Schutzzielen der Informationssicherheit und des Datenschutzrechts müssen technische und organisatorische Maßnahmen geprüft und festgelegt werden?

Antwort: Werden personenbezogene Daten verarbeitet, ergibt sich die Anwendung der Schutzziele unmittelbar aus dem SächsDSG (§ 9 Abs. 2 SächsDSG). Neben diesen Schutzzielen sind dabei auch die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten. Werden andere als personenbezogene Daten verarbeitet, sind die in § 9 Abs. 2 SächsEGovG genannten Schutzziele zu beachten.

Frage 5: Besteht die Verpflichtung für staatliche Behörden und Träger der Selbstverwaltung, Datenschutz- und Informationssicherheitskonzepte zu erstellen und zu pflegen, auch für bereits im Einsatz befindliche »Altverfahren«, mit denen personenbezogene Daten verarbeitet werden?

Antwort: Für bereits im Einsatz befindliche »Altverfahren« müssten entsprechend den Regelungen in § 10 SächsDSG ein Verfahrensverzeichnis geführt und ggf. eine Vorabkontrolle durchgeführt worden sein. Damit wurde bereits zum jetzigen Zeitpunkt die Zulässigkeit des Einsatzes des Verfahrens festgestellt und die zum Schutz der personenbezogenen Daten erforderlichen technischen und organisatorischen Maßnahmen getroffen. Gemäß § 5 Abs. 1 SächsEGovG sind für neu einzuführende Verfahren Datenschutz- und Informationssicherheitskonzepte zur Gewährleistung des Datenschutzes zu erstellen und zu pflegen. Diese sind vor der Inbetriebnahme des Verfahrens im Zusammenhang mit der Erstellung des Verfahrensverzeichnisses oder der Durchführung der Vorabkontrolle zu erstellen. Für bereits im Einsatz befindliche sogenannte »Altverfahren« sind die Datenschutz- und Informationssicherheitskonzepte sukzessive zu erstellen. Zu beachten ist jedoch, dass gemäß § 10 Abs. 4 SächsDSG Vorabkontrollen zwingend auch vor wesentlichen Änderungen von »Altverfahren« durchzuführen sind.

Frage 6: Welche Informationsmaterialien können für die Beantwortung von Datenschutzfragen im Zusammenhang mit der Erstellung von Datenschutzkonzepten neben den bereits im Textteil genannten Orientierungshilfen noch herangezogen werden?

Antwort: Hilfreich sind vor allem die im Internet veröffentlichten Tätigkeitsberichte des Sächsischen Datenschutzbeauftragten, die neben allgemeinen Hinweisen z. B. zur Durchführung von Vorabkontrollen, zur Führung des Verfahrensverzeichnisses, zu technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes auch zahlreiche Themen aus der Anwendungspraxis enthalten. Im Übrigen wird auf die Website des BSI verwiesen, insbesondere auf die übergreifenden Aspekte in den Bausteinen zum IT-Grundschutz.

§ 7 SächsEGovG – Barrierefreiheit

§ 7 SächsEGovG lautet:

»Die staatlichen Behörden und die Träger der Selbstverwaltung gestalten die elektronische Kommunikation und die elektronischen Dokumente schrittweise so, dass sie auch von Menschen mit Behinderung grundsätzlich uneingeschränkt und barrierefrei nach § 3 des Gesetzes zur Verbesserung der Integration von Menschen mit Behinderungen im Freistaat Sachsen (Sächsisches Integrationsgesetz – SächsIntegrG) vom 28. Mai 2004 (SächsGVBl. S. 196), das durch Artikel 14 des Gesetzes vom 14. Juli 2005 (SächsGVBl. S. 167, 176) geändert worden ist, in der jeweils geltenden Fassung, genutzt werden können.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung tritt unmittelbar nach Verkündung des SächsEGovG in Kraft. Sie gilt für die Träger der Selbstverwaltung (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG) seit dem 9. August 2014.

Inhalt der Verpflichtung

Nach dem Übereinkommen der Vereinten Nationen vom 13. Dezember 2006 über die Rechte von Menschen mit Behinderungen (UN-BRK) ist der Gesetzgeber verpflichtet, alle geeigneten Maßnahmen zu ergreifen, um Menschen mit Behinderungen einen gleichberechtigten Zugang zur öffentlichen Verwaltung zu schaffen und ihnen eine selbstbestimmte Teilhabe an allen modernen Informations- und Kommunikationstechnologien, die elektronisch bereit gestellt werden oder zur Nutzung offen stehen, zu ermöglichen. Dabei sind vorhandene Zugangshindernisse und -barrieren zu beseitigen (vgl. Art. 4, 9 und 21 UN-BRK).

Die bereits in § 7 SächsIntegrG verankerte Verpflichtung zur Barrierefreiheit ist zwar schon derzeit bei einem elektronischen Zugang als Teil des Internetauftritts der Behörde verpflichtend. § 7 SächsIntegrG gilt aber dann nicht, wenn eine Behörde einen Zugang über eine andere elektronische Möglichkeit – unabhängig vom Internet – wählt, beispielsweise bei Bezahlmöglichkeiten, Akteneinsicht oder Verwaltungspostfächern. Mit der Regelung in § 7 SächsEGovG soll in Verbindung mit § 1 Abs. 1 SächsEGovG daher zum einen eine barrierefreie Zugangseröffnung gewährleistet werden, die sowohl die elektronische Kommunikation der Verwaltung mit dem behinderten Bürger als auch zwischen den Verwaltungen ermöglicht.

Des Weiteren sind auch alle elektronischen Dokumente, also insbesondere digitale Unterlagen wie elektronische Formulare oder E-Mails so zu gestalten, dass sie für Menschen mit Behinderungen in der allgemein üblichen Weise ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind. Sofern die Verpflichtung mit Inkrafttreten der Norm noch nicht oder nur teilweise in bestimmten Verwaltungsverfahren erfolgt ist, haben die Träger der Selbstverwaltung die notwendigen Maßnahmen schrittweise, d. h. aufeinander folgend, zu treffen und umzusetzen, um überall dort, wo die Betroffenen miteinander Nachrichten austauschen oder elektronische Dokumente verwenden, noch bestehende Barrieren zu beseitigen. Dazu ist insbesondere ein Konzept zu erstellen, in dem terminlich untersetzt ist, welche Maßnahmen für die Umsetzung der Barrierefreiheit wann angegangen werden.

B Empfehlungen zur Umsetzung

Nach § 3 SächsIntegrG sind barrierefrei u. a. Systeme der Informationsverarbeitung, akustische und visuelle Informationsquellen und Kommunikationseinrichtungen sowie andere gestaltete Lebensbereiche, wenn sie für Menschen mit Behinderungen in der allgemein üblichen Weise ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind.

Barrierefreiheit bezieht sich auf die Gestaltung elektronischer Kommunikation im Allgemeinen (z. B. E-Mail-Verkehr, Internetangebote), aber auch auf die Gestaltung angehängter oder eingebetteter PDF-Dokumente(z. B. Formulare, Gesetzestexte). Hierfür gibt es internationale Standards, deren Einhaltung empfohlen wird.

B.1 Standards für Barrierefreiheit

B.1.1 WCAG

Der international anerkannte Standard für barrierefreie Webinhalte ist in den WCAG (engl.: **Web Content Accessibility Guidelines**) festgeschrieben. Danach folgen barrierefreie Webinhalte vier Prinzipien:

Wahrnehmbar (perceiveable)

Alle Inhalte sind für jeden wahrnehmbar. Es gilt das Zwei-Sinne-Prinzip: alle Informationen sind immer auf mehreren Wegen zugänglich. Ein Beispiel aus der Praxis ist die Haltestellenanzeige im Bus, die nicht nur angezeigt, sondern auch angesagt wird.

Bei Texten und Grafiken gilt vor allem, dass ausreichend Kontrast vorhanden ist, dass die Inhalte skalierbar sind (Zoom) und dass Grafiken mit einem beschreibenden Alternativtext versehen sind. Der Kontrast ist vor allem für Sehbehinderte wichtig, die sich die Farbe oft individuell einstellen.

Bedienbar (operable)

Inhalte dürfen nicht nur über die Maus oder ein Touchpad zugänglich sein, da dafür funktionierende Gliedmaßen erforderlich sind. Es gilt also auch, die Spracheingabe zu ermöglichen und die Tastaturbedienbarkeit sicherzustellen (Tab-Taste, Cursor-Tasten). Allgemein sind Seiten, die eine Bedienung über die Tastatur erlauben, auch über Spracheingabe oder eine Kommandozeilen-Schnittstelle zugänglich.

Verständlich (understandable)

Bei der Verständlichkeit wird in zwei Ebenen unterschieden. Die erste Ebene ist eine einfache Sprache, die z. B. Fachtexte auch für Laien zugänglich macht. Für Menschen mit kognitiven Einschränkungen gibt es die leichte Sprache.

Ebenfalls in die Rubrik fällt die Gebärdensprache, die einem anderen semantischen und syntaktischen Aufbau folgt. Gehörlose Menschen können dieser Sprache einfacher und schneller folgen.

Dieses Prinzip beschreibt vor allem die Notwendigkeit für Programme, damit assistive Technologien (siehe dazu die entsprechende Wikipedia-Definition) unterstützt werden.

Robust (robust)

Zur Robustheit zählt ebenso, dass Programme semantische Auszeichnungen wie Überschriften und Absätze auslesen beziehungsweise erstellen können.

Grundsätzlich gilt also, dass Dokumente und Programme so beschaffen sein müssen, dass Menschen mit Behinderungen sie nach ihren individuellen Bedürfnissen nutzen können. Ausschlaggebend ist hierbei, dass sie das grundsätzlich »in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe« können.

B.1.2 PDF/UA

Für **PDF-Dokumente** gilt international der auf Basis der WCAG entwickelte Standard PDF/UA (engl.: **Universal Accessibility**). Dieser Standard wurde inzwischen als DIN ISO 14289-1:2014-02 veröffentlicht.

B.1.3 BITV 2.0

Auf nationaler Ebene hat die **BITV 2.0** (**Barrierefreie-Informations-Technik-Verordnung des Bundes**) Maßstäbe für die Gestaltung eines barrierefreien Internets gesetzt. Die WCAG-Prinzipien sind vollständig in die BITV 2.0 aufgenommen worden und gelten damit unmittelbar für die Bundesverwaltung.

Darüber hinaus nimmt die BITV 2.0 Differenzierungen vor, indem sie bei der Berücksichtigung von Behinderungen nach Prioritäten unterscheidet:

- Der Kriterienkatalog der Priorität 1 berücksichtigt im Wesentlichen die Anforderungen blinder und sehbehinderter Menschen an einen barrierefreien Internetzugang.
- Die Kriterien der Priorität 2 berücksichtigen die Anforderungen gehörloser und hörbehinderter Menschen sowie von Menschen mit kognitiven Einschränkungen.

Tipp

Es wird grundsätzlich empfohlen, sich bei der Gestaltung von Internetauftritten und Dokumenten an diesen drei Standards zu orientieren, da sie eindeutig und nachvollziehbar sind und damit auch die Vergleichbarkeit von Angeboten nach Ausschreibungen sicherstellen.

Darüber hinaus haben diese Standards sich international durchgesetzt, stellen den Stand der Technik dar, werden von den deutschen Behindertenverbänden mitgetragen und auch in Sachsen, z. B. von der Sächsischen Staatskanzlei bei der Weiterentwicklung der Website www.sachsen.de, berücksichtigt.

B.2 Externe Vergabe von Webangeboten

Die folgende Formulierung wird bei Ausschreibungen der Neugestaltung von Internetauftritten und der elektronischen Kommunikation empfohlen: »Die ausgeschriebenen Leistungen, sind den Anforderungen der BITV 2.0 und der PDF/UA gemäß barrierefrei zu erstellen. Der Dienstleister / die Agentur weist entsprechende Erfahrung bei der Erstellung barrierefreier Webauftritte / PDF-Dokumente nach.«

Die Sicherstellung der Einhaltung der genannten Standards obliegt dem ausschreibenden Träger der Selbstverwaltung. In Sachsen übernimmt unter anderem die Deutsche Zentral-

bücherei für Blinde in Leipzig (DZB) die Überprüfung von Internetseiten hinsichtlich der Erfüllung der Standards nach BITV 2.0. Es gibt aber auch freie Anbieter.

B.3 Prüfung von Internetangeboten

Wenn ein Träger der Selbstverwaltung Internetangebote bereithält oder neue ausschreibt, ist fortan sicherzustellen, dass diese barrierefrei sind. Dies geschieht über ein Prüfprotokoll.

Grundlage der Prüfung ist die Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV 2.0). Das Projekt BIK – barrierefrei informieren und kommunizieren, ein Gemeinschaftsprojekt zweier Verbände der Behindertenselbsthilfe und der DIAS GmbH, hat einen Test nach BITV entwickelt und Prüfschritte definiert. Insgesamt wird die Einhaltung von 50 Anforderungen überprüft.

Das Verzeichnis der Prüfschritte ist online publiziert. Üblicherweise wählt der Prüfer aus einem Internetangebot eine Reihe von Einzelseiten aus, die anhand der Kriterien getestet werden. Aus dem abschließenden Prüfbericht lassen sich Maßnahmen zur Optimierung des Internetangebotes ableiten. Auch ein Selbsttest ist möglich.

Elektronische Dokumente wie Broschüren oder Vordrucke sollten auf Konformität mit dem PDF/UA-Standard, dem Standard der PDF Association für barrierefreie PDF geprüft werden. Für die Prüfung von Dokumenten gilt das Matterhorn Protokoll 1.0 als Prüfkatalog. Das Matterhorn Protokoll enthält 31 Prüfbereiche und 136 Fehlerbedingungen, die nach Prüfung durch Software und Prüfung durch eine Person unterschieden werden.

B.4 Dienstleister zur Erstellung und Zertifizierung barrierefreier Webseiten

Die aufgeführten Adressen erheben keinen Anspruch auf Vollständigkeit.

B.4.1 Prüfung nach BITV-Standard

Deutsche Zentralbücherei für Blinde
Gustav-Adolf-Straße 7
04105 Leipzig
Tel: 0341 7113-0
Fax: 0341 7113-125
E-Mail: info@dzb.de
Web: www.dzb.de

BIK Testentwicklung c/o DIAS GmbH
Schulterblatt 36
20357 Hamburg
Tel: 040 431875-0
Fax: 040 431875-19
E-Mail: kontakt@bik-online.info
Web: www.dias.de

B.4.2 Vermittlung von Gebärdensprachdolmetschern, auch für die Erstellung von Videos

Landesdolmetscherzentrale für Gebärdensprache
Ebersbrunner Straße 25
08064 Zwickau
Tel: 0375 77044-0
Fax: 0375 77044-10
E-Mail: info@ldz-zwickau.de
Web: www.gehoerlosenzentrum-zwickau.de/Landesdolmetscherzentrale-fuer-Gebaerdensprache.html

Berufsverband der Gebärdensprachdolmetscher/innen Sachsen e.V. (BVGS e.V.)
Fritz-Reuter-Straße 34a
01097 Dresden
Tel: 0176 201988-63
E-Mail: 1.Vorsitzender@bvg-sachsen.de
Web: www.bvg-sachsen.de/dolmetscher-finden

B.4.3 Erstellung und Zertifizierung von Texten in Leichter Sprache

Verein »Netzwerk Leichte Sprache«
Tel: 0251 98796-87
E-Mail: info@leichtesprache.org
Web: www.leichtesprache.org

Büro für Leichte Sprache
Lebenshilfe Landesverband Sachsen e.V.
Heinrich-Beck-Straße 47
09112 Chemnitz
Tel: 0371 90991-0
Fax: 0371 90991-11
E-Mail: information@lebenshilfe-sachsen.de
Web: www.inklusion-in-sachsen.de

Leben mit Handicaps e. V.
c/o Institut für psychosoziale Gesundheit
Frau Dr. Marion Michel
Schenkendorfstraße 27
04275 Leipzig
Tel: 0341 3068182
E-Mail: info@leben-mit-handicaps.de

Stiftung Universität Hildesheim
Institut für Übersetzungswissenschaft und Fachkommunikation
Frau Prof. Dr. Christiane Maaß
Geschäftsführende Direktorin
Lübecker Straße 3
31141 Hildesheim
Tel: 05121 88330-900
E-Mail: leichte.sprache@uni-hildesheim.de

B.4.4 Schulungen zur Gestaltung barrierefreier Webauftritte und PDF-Dokumente

Die AVS Meißen bietet **Seminare für Online-Redakteure** und **Seminare zur Gestaltung barrierefreier PDF-Dokumente** an. Es ist vorgesehen, das Fortbildungsangebot zum Thema »Barrierefreiheit« im Zuge der Umsetzung des SächsEGovG weiterzuentwickeln.

Akademie für öffentliche Verwaltung
Herr Jens Weckbrodt
Lehrgangsplanung
Herbert-Böhme-Straße 11
01662 Meißen
Tel: 03521 473-717
Fax: 03521 473-707
E-Mail: jens.weckbrodt@avs.sachsen.de

Nach Verfügbarkeit und Absprache werden Plätze in Seminaren auch an Mitarbeiter von Kommunen vergeben. Die AVS steht für diesbezügliche Anfragen zur Verfügung.

B.5 Weiterführende Informationen

- Handreichung für Agenturen zu den Anforderungen an barrierefreie PDF-Dokumente des Sächsischen Staatsministeriums für Soziales und Verbraucherschutz
- Webseiten der PDF-Associaton zum Stand barrierefreier PDF-Dokumente
- Beispiele barrierefreier Websites:
  - http://www.bmas.de/DE/Startseite/start.html
  - http://www.behindertenbeauftragte.de/DE/Home/home_node.html
  - http://v1.bitv-test.de/index.php?a=ti&sid=1051
  - http://www.baden-wuerttemberg.de/de/startseite/
  - http://www.skd.museum/
- Das Projekt BIK »barrierefrei kommunizieren und informieren« veröffentlicht von ihm nach BITV 2.0-Standard geprüfte Webangebote, Agenturen und Redaktionssysteme (CMS) in der Liste 90plus. Die geprüften Anbieter erfüllen mehr als 90% der Anforderungen der BITV 2.0. Auch die Prüfberichte sind dort veröffentlicht.

C Beantwortung häufig gestellter Fragen

Frage 1: Wo kann ich das im SächsEGovG genannte Sächsische Integrationsgesetz einsehen?

> **Antwort**: Sie können sich das Sächsische Integrationsgesetz in der aktuellen Fassung im Internet herunterladen.

Frage 2: Wo erhalte ich konkrete Hinweise zur barrierefreien Gestaltung elektronischer Kommunikation und elektronischer Dokumente?

> **Antwort**: Die für Behörden der Bundesverwaltung verpflichtende »Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0)« enthält detaillierte

Vorgaben. Es wird empfohlen, sich an diesem Standard zu orientieren. Darüber hinaus bietet z. B. die Website »Einfach für Alle« der »Aktion Mensch« umfangreiche Informationen und Anleitungen zu speziellen Themen.

Frage 3: An wen wende ich mich, wenn ich feststelle, dass bei einer der eingebundenen Basiskomponenten Barrieren für Menschen mit Behinderungen bestehen?

Antwort: Bitte wenden Sie sich in diesem Fall an den jeweiligen Verantwortlichen für die Basiskomponente.

Frage 4: Welche gesetzlichen Grundlagen gelten für Internetseiten und Internetangebote in Form von elektronischen Formularen, Vordrucken und Dokumenten?

Antwort: Maßgeblich für Internetangebote der Träger öffentlicher Gewalt ist das Gesetz zur Gleichstellung behinderter Menschen von 2002 (BGG) und das Gesetz zur Verbesserung der Integration von Menschen mit Behinderungen im Freistaat Sachsen (SächsIntegrG).

Frage 5: In welchem Zeitraum müssen Internetangebote an die Anforderungen der Barrierefreiheit angepasst werden?

Antwort: Das SächsEGovG gibt keine Fristen vor. Allerdings fordert das Gesetz eine schrittweise Umsetzung, was bedeutet, dass mit der Umsetzung unmittelbar begonnen werden muss.

Frage 6: Für welche Gruppen von Menschen mit Behinderungen sind typischerweise Vorkehrungen zu treffen, damit ein barrierefreier Zugang und eine barrierefreie Nutzung elektronischer Kommunikation möglich sind?

Antwort: Insbesondere für Menschen mit Sehbehinderungen, für blinde und gehörlose Menschen sowie für Menschen mit kognitiven Behinderungen sind bestimmte Vorkehrungen erforderlich. Für Menschen mit motorischen Einschränkungen sind Fragen der Bedienbarkeit (vgl. Abschnitt B.1.1) von Bedeutung. Darüber hinaus verbessern barrierefreie Dokumente auch für nicht-behinderte Menschen die Bedienbarkeit – insbesondere bei der Nutzung mobiler Endgeräte.

Frage 7: In welchem Umfang sind Vorkehrungen zu treffen?

Antwort: Einen Orientierungspunkt hierfür gibt die (für den Bund verbindliche) Barrierefreie-Informationstechnik-Verordnung 2.0 (BITV 2.0). Konkret verweist deren § 3 und ihre Anlagen auf anzuwendende Standards.
Darüber hinaus ist darauf zu achten, dass im PDF gespeicherte Dokumente so strukturiert sind, damit assistiven Technologien (siehe dazu die entsprechende Wikipedia-Definition) der Zugang zu den Inhalten gewährleistet wird, vgl. ISO-Standard PDF/UA für universelle Barrierefreiheit.

Frage 8: Hat ein behinderter Mitarbeiter eines Landratsamtes bei Durchführung eines Verwaltungsverfahrens mit einer Gemeinde aus §§ 7, 2 Abs. 1 i. V. m. § 1 Abs. 1 SächsEGovG einen Anspruch darauf, dass ihr der entsprechend zuständige Mitarbeiter der Gemeindeverwaltung beispielsweise eine dafür notwendige E-Mail barrierefrei zusendet?

> **Antwort**: Nein. Aus § 7 SächsEGovG folgt kein Rechtsanspruch eines Verwaltungsmitarbeiters auf eine barrierefreie elektronische Kommunikation mit einer anderen Behörde / Träger der Selbstverwaltung oder einem Dritten. Die Verpflichtung, die elektronische Kommunikation barrierefrei zu gestalten, hat objektivrechtlichen Charakter und richtet sich damit unmittelbar an den Verwaltungsträger und nicht an den Bürger. Sie ist zwar insofern drittschützend, dass sie ausschließlich dazu dient, den Menschen mit Behinderung die elektronische Kommunikation zu den Verwaltungsverfahren und beim Verwaltungshandeln der Behörden und sonstigen öffentlichen Stellen zu ermöglichen. Dies dient aber in erster Linie damit der effizienten Erledigung der Verwaltungsaufgaben der Behörde / des Trägers der Selbstverwaltung selbst. Die Norm überlässt der Verwaltung zudem einen Gestaltungsspielraum wie und vor allem wann die Barrierefreiheit bei der elektronischen Kommunikation umgesetzt wird. Insofern benennt das Gesetz keine hinreichend konkreten Maßnahmen, die im Einzelfall Gegenstand eines Anspruchs sein könnten.

Frage 9: Wie ist Frage 8 zu beantworten, wenn die Behörden die elektronische Vorgangsbearbeitung und Aktenführung eingeführt haben?

> **Antwort**: In diesem Fall sind die Verfahren barrierefrei nach § 12 Abs. 6 SächsEGovG so zu gestalten, dass sie auch von Mitarbeitern, die mit der elektronischen Akte arbeiten müssen, grundsätzlich uneingeschränkt genutzt werden können. Auch hier verbleibt den Behörden ein Gestaltungsspielraum, wie die behördeninterne und -übergreifende Barrierefreiheit konkret gewährleistet wird.

Frage 10: Wie kann ich sicherstellen, dass meine Internetangebote barrierefrei sind?

> **Antwort**: Sie können Ihre Internetangebote nach den Prüfkriterien der BITV im Selbsttest oder bei externen Anbietern (vgl. Adressliste im Abschnitt B.4) prüfen. Als barrierefrei gilt, wenn mindestens 90 % der Kriterien erfüllt sind. Die externe Prüfung wird empfohlen.

§ 13 Abs. 1 SächsEGovG – Informationssicherheit

§ 13 Abs. 1 SächsEGovG lautet:

»Für die am E-Government beteiligten Träger der Selbstverwaltung gilt § 9 Abs. 2 S. 1 und 2 entsprechend.«

§ 9 Abs. 2 SächsEGovG lautet:

»Die staatlichen Behörden treffen angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zur Einhaltung der in § 9 Abs. 2 SächsDSG definierten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz für die in ihren informationstechnischen Systemen verarbeiteten Daten. Solche Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen einer Verletzung der Schutzziele steht. Zur Erreichung und Aufrechterhaltung dieses Informationssicherheitsniveaus sind für die staatlichen Behörden die Standards und Kataloge des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuellen Fassung maßgeblich.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung tritt unmittelbar nach Verkündung des SächsEGovG in Kraft. Sie gilt für die Träger der Selbstverwaltung (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG) seit dem 9. August 2014.

Adressat der Verpflichtung

Die in § 9 Abs. 2 S. 1 und S. 2 SächsEGovG festgeschriebene Verpflichtung richtet sich laut § 13 Abs. 1 SächsEGovG an alle am E-Government teilnehmenden Träger der Selbstverwaltung in Sachsen, da diese für die Einhaltung der im SächsDSG definierten Schutzziele und für die Gewährleistung eines entsprechenden Informationssicherheitsniveaus selbst verantwortlich sind. Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für den Datenschutz und die Informationssicherheit hat die Leitung der Behörde oder Einrichtung. Sie oder die vorgesetzte Dienstbehörde erlässt die erforderlichen Regelungen für den Bereich der Behörde. Die aktuellen Regelungen sind den Beschäftigten bekannt zu geben.

Sofern benannt, können der Datenschutzbeauftragte oder der Beauftragte für Informationssicherheit der jeweiligen Behörde oder Einrichtung die Behördenleitung bei der Umsetzung der in § 9 Abs. 2 SächsEGovG genannten Verpflichtung unterstützen.

Geltungsbereich der Verpflichtung

Die Verpflichtung gilt für die am E-Government teilnehmenden Träger der Selbstverwaltung (zum Begriff Träger der Selbstverwaltung siehe die Ausführungen oben zu § 2 Abs. 1 SächsEGovG). Nicht verpflichtend sind für die Träger der Selbstverwaltung die in § 9 Abs. 2 S. 3 SächsEGovG genannten Standards und Kataloge des BSI, die nur die Staatsverwaltung binden.

Inhalt der Verpflichtung

§ 13 Abs. 1 SächsEGovG schreibt für die Träger der Selbstverwaltung, die am E-Government teilnehmen, die Absicherung eines angemessenen Informationssicherheitsniveaus für ihre eingesetzten informationstechnischen Systeme vor, so wie es § 9 Abs. 2 S. 1 und 2 SächsEGovG für die staatlichen Behörden fordert.

Unter E-Government versteht man den Einsatz elektronischer Informationstechnologien, um die Services der Behörden für Bürger und Unternehmen einfach und schnell zugänglich zu machen. E-Government dient dem Informationsaustausch zwischen Behörden und Bürgern sowie Unternehmen, aber auch zwischen und innerhalb von Behörden. Das kann der Austausch von Formularen, Informationen oder Akten sein, das Stellen oder Bearbeiten eines Antrags oder einfach nur der Blick auf die Internetseite einer Behörde, um sich über Öffnungszeiten oder benötigte Formulare zu informieren.

Sind die Träger der Selbstverwaltung in diesem Sinne am E-Government mit einer oder mehreren E-Government-Anwendungen beteiligt, müssen sie die entsprechenden im Einsatz befindlichen informationstechnischen Systeme und Prozesse so gestalten, dass die Daten, die verarbeitet werden, vor unbefugter oder unsachgemäßer Nutzung geschützt, d. h. sicher, sind. Dies ist praktisch schon immer deshalb der Fall, da spätestens mit Inkrafttreten des § 2 Abs. 1 SächsEGovG die Verpflichtung besteht, den Zugang für die elektronische Kommunikation zu eröffnen. Wie der Schutz zu erfolgen hat und welche Schutzziele dafür gelten regelt sich nach § 9 Abs. 2 S. 1 SächsEGovG.

§ 9 Abs. 2 S. 1 SächsEGovG benennt ausdrücklich die relevanten Informationssicherheitsziele und verweist auf die in § 9 Abs. 2 SächsDSG enthaltenen Legaldefinitionen hierzu.

Die Anforderungen des § 9 Abs. 2 S. 1 SächsEGovG weichen dabei jedoch von den Vorgaben des § 9 Abs. 2 SächsDSG inhaltlich ab. Während letzteres dem Datenschutz gewidmet ist, normiert § 9 Abs. 2 S. 1 SächsEGovG Fragen der Informationssicherheit. Entsprechend geht diese Regelung über die in § 9 Abs. 2 SächsDSG enthaltene Verpflichtung hinaus, da dort nur Regelungen für personenbezogene Daten enthalten sind. Demgegenüber werden hier Anforderungen für alle Daten in den informationstechnischen Systemen der staatlichen Behörden getroffen. Dies gilt sowohl für Daten, die bei der Verarbeitung im selbstverwalteten als auch im übertragenen Aufgabenbereich anfallen. Daher ist nun über den konkreten Personenbezug hinaus für alle Daten zu gewährleisten, dass

- nur Befugte Daten zur Kenntnis nehmen können (Vertraulichkeit);
- Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität);
- Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit);
- jederzeit Daten ihrem Ursprung zugeordnet werden können (Authentizität);
- festgestellt werden kann, wer wann welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) und dass
- die Verfahrensweisen bei der Verarbeitung Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

§ 9 Abs. 2 S. 2 SächsEGovG konkretisiert die in § 9 Abs. 2 S. 1 SächsEGovG enthaltene Vorgabe »angemessene[r] [...] Vorkehrungen«, indem diese Angemessenheit näher beschrieben wird. Für die verschiedenen, von den staatlichen Behörden einzusetzenden informationstechnischen Systeme ist danach für alle sechs in § 9 Abs. 2 S. 1 SächsEGovG benannten Schutzziele die Notwendigkeit von Schutzmaßnahmen zumindest zu prüfen. Allerdings können bei konkreten informationstechnischen Systemen einzelne Schutzziele lediglich so geringfügig betroffen sein, dass jegliche Schutzmaßnahmen für sie unverhältnismäßig aufwendig wären. In diesen Fällen ergibt sich allein aus der Nennung der sechs Schutzziele in § 9 Abs. 2 S. 1 SächsEGovG keine Notwendigkeit stets für alle benannten Ziele Schutzmaßnahmen vorzusehen. Vielmehr ist es zur Wahrung der Pflichten aus § 9 Abs. 2 S. 1 und S. 2 SächsEGovG ausreichend für die tatsächlich substantiell betroffenen Schutzziele angemessene Schutzmaßnahmen vorzusehen.

B Empfehlungen zur Umsetzung

Eine wesentliche Grundlage für die Umsetzung der in § 13 Abs. 1 i. V. m. § 9 Abs. 2 SächsEGovG geforderten Einhaltung der in § 9 Abs. 2 SächsDSG definierten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz bilden die Standards und Kataloge des BSI. Diese im SächsEGovG als maßgeblich für die staatlichen Behörden festgelegten Standards und Kataloge (kurz BSI-Grundschutz) sind sehr umfangreich und bieten ein generisches Vorgehensmodell zur Erreichung eines angemessenen Informationssicherheitsniveaus. Dazu können aus einer Vielzahl von personellen, technischen, organisatorischen und infrastrukturellen Sicherheitsmaßnahmen diejenigen ausgewählt werden, die den Schutzbedarf der jeweiligen Behörde oder Einrichtung am besten abdecken. Sie gelten allerdings nicht direkt und unmittelbar für die Träger der Selbstverwaltung.

Obwohl BSI-Grundschutz einen hohen Vollständigkeitsanspruch bzgl. des sehr vielschichtigen Themas Informationssicherheit hat, wird auf der anderen Seite oft beklagt, dass gerade dadurch die Übersichtlichkeit und Anwendbarkeit für kleinere Einrichtungen leidet. Das war auch der Grund dafür, dass die 2012 von der SAKD veröffentlichte »Musterleitlinie zur Herstellung und Gewährleistung der Informationssicherheit in sächsischen Kommunalverwaltungen« keine Anwendung von BSI-Grundschutz vorgibt.

Für staatliche Behörden ist die Anwendung von BSI-Grundschutz bereits seit 2011 mit der VwV Informationssicherheit als maßgeblich festgelegt und jetzt mit § 9 Abs. 2 S. 3 SächsEGovG auch gesetzlich geregelt. Da aber auch die SAKD die Orientierung an BSI-Grundschutz als Praxisleitfaden vorschlägt, wird für alle Träger der Selbstverwaltung das im Folgenden beschriebene parallele Vorgehen empfohlen. Parallel meint hier, einerseits das formelle und gesetzlich vorgeschriebene Vorgehen nach BSI konsequent anzugehen, anderseits aber auch das Tagesgeschäft zur praktischen Abwehr von Informationssicherheitsrisiken nicht zu vernachlässigen. Aufgrund der oft angespannten personellen Situation in den Behörden und Einrichtungen kann das nur durch die Unterstützung der Leitungsebene und durch eine Priorisierung der Maßnahmen gelingen.

B.1 Umsetzung BSI-Grundschutz

Wesentliche Voraussetzung für das Erreichen eines angemessenen Informationssicherheitsniveaus ist nicht nur laut BSI-Grundschutz in jedem Fall die Schaffung der organisatorischen Grundlagen. Dafür sollte – wenn nicht bereits vorhanden – zuerst eine Leitlinie für

Informationssicherheit für die jeweilige Behörde oder Einrichtung erarbeitet werden. In der Leitlinie muss festgeschrieben werden,

- dass die Leitungsebene die unteilbare Verantwortung für die Informationssicherheit hat,
- welche Ziele und Strategien mit der Informationssicherheit verfolgt werden,
- wie die organisatorischen Strukturen aufgebaut werden,
- dass ausreichende Ressourcen für die Umsetzung der Ziele bereitgestellt werden und
- dass alle Mitarbeiter in den Informationssicherheitsprozess eingebunden werden.

Für alle operativen und koordinierenden Belange und Fragen der Informationssicherheit – also z. B. auch die Koordinierung der Erstellung und Verabschiedung der Leitlinie – kann und sollte in jeder Behörde oder Einrichtung ein Beauftragter für Informationssicherheit (BfIS) benannt werden. Für alle obersten Landesbehörden ist das bereits mit der VwV Informationssicherheit als Pflicht festgelegt.

Für eine detaillierte Darstellung des Vorgehens zum Aufbau eines Informationssicherheitsmanagements wird auf die entsprechenden Webseiten des BSI verwiesen.

Als Vorlage für eine eigene Leitlinie können die kommunalen Behörden auf die »Musterleitlinie zur Herstellung und Gewährleistung der Informationssicherheit in sächsischen Kommunalverwaltungen« der SAKD zurückgreifen, die auf den Regelungen der VwV Informationssicherheit des Landes basiert.

Weitere Quellen können die entsprechenden Webseiten des BSI oder die vom IT-Planungsrat verabschiedete »Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung« sein.

Mit der Verabschiedung einer eigenen Leitlinie und dem Aufbau der darin geregelten organisatorischen Strukturen inkl. der entsprechenden Ressourcenbereitstellung ist bereits ein wichtiger Schritt für die Umsetzung der im SächsEGovG (und auch im SächsDSG) geforderten Einhaltung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz geschafft. Aufbauend auf dieser Grundlage können dann die weiteren Schritte laut BSI-Grundschutz angegangen werden. Das sind:

- Entwicklung eines Sicherheitskonzepts gemäß IT-Grundschutz-Vorgehensweise,
- Umsetzung durch Beseitigung vorhandener Schwachstellen und Einführung der im Konzept vorgesehenen Maßnahmen,
- Aufrechterhaltung und kontinuierliche Verbesserung durch Prüfung von Wirksamkeit, Angemessenheit und Aktualität der vorhandenen Konzepte und eingeführten Maßnahmen.

Für eine genauere Auflistung der damit verbundenen Arbeiten wird auf die Website des BSI zum Thema IT-Grundschutz verwiesen.

Einen guten und kompakten Überblick zum Einstieg in das Thema BSI-Grundschutz bietet auch der Leitfaden Informationssicherheit des BSI.

B.2 Wichtige Sofortmaßnahmen

Neben dem Aufsetzen des Sicherheitsprozesses laut BSI-Grundschutz muss parallel darauf geachtet werden, dass auch die bereits etablierten Sicherheitsmaßnahmen nicht vernachlässigt, sondern im Gegensatz ständig überprüft und weiter verbessert werden müssen. Dabei verfügen die an das KDN angeschlossenen kommunalen Behörden bereits über einen guten Basisschutz, da sie durch die Standardsicherheitsmaßnahmen des SVN und des KDN mit geschützt werden.

Kommunalen Behörden, die noch nicht an das KDN angeschlossen sind, wird als **wichtigste Sofortmaßnahme zur Gewährleistung eines angemessenen Informationssicherheits-niveaus die Prüfung des Anschlusses an das KDN** empfohlen. Genauere Ausführungen finden sich dazu auch in den FAQs zu § 15 SächsEGovG.

Hintergrund der Empfehlung des KDN-Anschlusses aus Sicht der Informationssicherheit ist das hohe Schutzniveau für die Teilnehmer innerhalb des vom Internet getrennten SVN-Verbunds. Die implementierten Schutzmaßnahmen des SVN und KDN wie hochwertige Schadsoftware-Scanner und moderne Angriffserkennungssysteme sind sehr wirkungsvoll (12.000 abgewehrte Angriffe, 1,5 Mrd. abgewiesene Spam-E-Mails, Ausfilterung von 175.000 Viren und 340.000 Schadprogrammen in den letzten 5 Jahren). Es ist schwer, ein vergleichbares Schutzniveau mit den oft angespannten finanziellen und personellen Ressourcen einer Kommune zu realisieren. Dazu kommt, dass die Schutzmaßnahmen des SVN und KDN ohne zusätzliche Kosten im KDN-Anschluss enthalten sind.

Folgende weitere Sofortmaßnahmen werden empfohlen.

- Alle Kommunen stellen, soweit möglich, die von ihnen betriebenen HTTPS-Seiten mit fehlerhaften Zertifikaten auf Zertifikate der Sachsen Global CA um. Alle Zertifikatsfehler werden beseitigt. Hierzu wird auf die Handlungsanleitungen zur Beantragung der Serverzertifikate für Apache und der Serverzertifikate für Microsoft IIS im Anhang zu diesem Handlungsleitfaden verwiesen.
- Die Kommunen prüfen die Möglichkeiten, verschlüsselte E-Mail-Kommunikation zwischen ihren Servern und denen ihrer Kommunikationspartner zu realisieren. Wo möglich wird die Verschlüsselungsoption STARTTLS für den serverseitigen E-Mail-Empfang und –Versand durchgängig umgesetzt. Auf die entsprechenden Ausführungen der SAKD und die technischen Tipps bei Heise Security wird verwiesen.
- Alle Kommunen stellen intern flächendeckend auf verschlüsselte Kommunikation zwischen den E-Mail-Clients und E-Mail-Servern um. Beispielhaft wird auf die Handlungsanleitung zur Verschlüsselung von Verbindungen zwischen Microsoft Outlook und Exchange im Anhang zu diesem Handlungsleitfaden verwiesen.
- Alle Kommunen schalten sofort die stark unsicheren Verschlüsselungsprotokolle SSLv2 und SSLv3 auf ihren Internetseiten und -diensten ab. Darüber hinaus werden kurzfristig weitere Maßnahmen zur Härtung der HTTPS-Konfiguration umgesetzt, die mit der HTTPS-Konfiguration für Apache und der HTTPS-Konfiguration für Microsoft IIS im Anhang zu diesem Handlungsleitfaden beschrieben sind.
- Berücksichtigung finden sollten auch die vom AK ITEG für die Landesverwaltung beschlossenen Handlungsempfehlungen und der Umsetzungsplan der AG IS zum verbesserten Einsatz von Verschlüsselungsverfahren im Anhang zu diesem Handlungsleitfaden.

Hintergrund der empfohlenen Sofortmaßnahmen ist der bestehende Handlungsbedarf im Bereich Verschlüsselung. Durch die hohe Komplexität des Themas und angespannte Ressourcen werden entsprechende Maßnahmen oft immer wieder verschoben, was im Ergebnis zu einem nicht angemessenen Informationssicherheitsniveau führt.

So ergab ein aktueller Lagebericht zum Stand des Einsatzes von Verschlüsselungsverfahren in den sächsischen Landes- und Kommunalverwaltungen, dass bei einer Vielzahl der HTTPS-Internetseiten und -dienste Verbesserungsbedarf besteht.

In Auswertung des Lageberichts hat die Landesverwaltung für ihren Bereich die in den obigen Sofortmaßnahmen genannten Handlungsempfehlungen beschlossen. Den Trägern der Selbstverwaltung wird empfohlen, entsprechende Regelungen auch für ihren Bereich zu verabschieden.

C Beantwortung häufig gestellter Fragen

Frage 1: Gibt es zeitliche Fristen für die Umsetzung der Vorgaben nach § 13 Abs. 1 i. V. m. § 9 Abs. 2 SächsEGovG?

> **Antwort**: Die Umsetzung muss im Rahmen der Eigenverantwortung der jeweiligen Behörde oder Einrichtung erfolgen. Konkrete zeitliche Vorgaben zur Umsetzung gehen aus dem SächsEGovG nicht hervor.

§ 15 SächsEGovG – Datenübermittlung

§ 15 Abs. 1 SächsEGovG lautet:

»Die verwaltungsebenenübergreifende elektronische Datenübermittlung im Sinne von § 11 zwischen den staatlichen Behörden und den Trägern der Selbstverwaltung wird über das Sächsische Verwaltungsnetz geführt. Die kommunalen Träger der Selbstverwaltung können dabei den Zugang zu dem Sächsischen Verwaltungsnetz über das Kommunale Datennetz und die nichtkommunalen Träger der Selbstverwaltung über einen unmittelbaren Anschluss herstellen. Alternativ können die Träger der Selbstverwaltung den Zugang zu dem Sächsischen Verwaltungsnetz über eine Schnittstelle herstellen, die eine vergleichbare Funktionalität und eine gleichwertige Informationssicherheit gewährleistet. Satz 1 gilt nicht, soweit für einzelne Fachverfahren spezielle Rechtsvorschriften eine zuverlässige und sichere Datenübermittlung gewährleisten.«

§ 15 Abs. 2 S. 1 SächsEGovG lautet:

»Die Staatsregierung wird ermächtigt, die Eigenschaften der Schnittstelle gemäß Absatz 1 Satz 3 durch Rechtsverordnung näher zu bestimmen, soweit dies zur Wahrung der Voraussetzungen des Absatzes 1 Satz 3 erforderlich ist.«

A Erläuterung der Verpflichtung

Inkrafttreten

Die Verpflichtung, für die elektronische Datenübermittlung zwischen Staatsbehörden und Trägern der Selbstverwaltung das Sächsische Verwaltungsnetz (SVN) zu benutzen, gilt für die Träger der Selbstverwaltung (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG) unmittelbar mit Inkrafttreten des Gesetzes seit dem 9. August 2014.

Inhalt der Verpflichtung

Nach § 11 SächsEGovG ist die elektronische Übermittlung von Daten in einer zur dauerhaften Wiedergabe geeigneten Form (elektronische Datenübermittlung) zwischen den staatlichen Behörden über ein informationstechnisches Netz zu führen, dass deren informationstechnische Netze verbindet (Sächsisches Verwaltungsnetz, SVN). Diese Pflicht zur Verwendung des SVN wird mit § 15 Abs. 1 SächsEGovG ausgedehnt, so dass auch die Datenübermittlung zwischen den staatlichen Behörden und den Trägern der Selbstverwaltung erfasst wird, soweit diese verwaltungsebenenübergreifend ist.

Das SächsEGovG definiert den Begriff »verwaltungsebenenübergreifend« nicht. Im Staatsaufbau des Freistaates unterscheidet man herkömmlich zwei Verwaltungsebenen. Den Freistaat (Staatsregierung und ihre nachgeordneten Behörden) und die Träger der Selbstverwaltung, wobei letztere wiederum in die Unterebenen Landkreise, Gemeinden und andere Gemeindeverbände unterteilt werden (vgl. Art. 82 Abs. 1 S. 1, Abs. 2 S. 1 SächsVerf). Erfolgt die elektronische Datenübermittlung also beispielsweise zwischen einem Zweckverband und der Landesdirektion, so erfolgt sie verwaltungsebenenübergreifend im Sinne des § 15 Abs. 1 SächsEGovG und hat über das SVN zu erfolgen.

Diese Pflicht zur elektronischen Datenübermittlung gilt jedoch nicht für den Bereich der Telefonie, weder im Mobilfunk- noch im Festnetz, und zwar selbst für den Fall, dass die

Sprachdaten durch Voice over IP (Übertragung der digitalisierten Sprachdaten über das Internet Protocol) über elektronische Netze übertragen werden. Diese Einschränkung ergibt sich aus der Verweisung in § 15 Abs. 1 S. 1 SächsEGovG für den Begriff der elektronischen Datenübermittlung auf § 11 SächsEGovG, in dem hierzu eine Legaldefinition enthalten ist: »die elektronische Übermittlung von Daten in einer zur dauerhaften Wiedergabe geeigneten Form«. Diese Formulierung orientiert sich am Wortlaut des § 126b BGB. Die Definition in § 11 SächsEGovG schließt lediglich die telefonische Kommunikation aus, nicht jedoch die elektronische Übermittlung von elektronischen Akten inklusive der darin eventuell enthaltenen Dokumente, die keine Schriftzeichen aufweisen, wie z. B. bildliche Darstellungen in Planungsunterlagen oder als Anlagen beigefügte Tondokumente. Die telefonische Kommunikation kann daneben zwar freiwillig von den Trägern der Selbstverwaltung auch über das SVN geführt werden. Eine Pflicht hierzu enthält § 15 Abs. 1 S. 1 SächsEGovG allerdings nicht.

Gemäß § 15 Abs. 1 S. 2 SächsEGovG können die kommunalen Träger der Selbstverwaltung ihre Anbindung an das SVN über das Kommunale Datennetz (KDN) herbeiführen, was empfohlen wird. Die nichtkommunalen Träger der Selbstverwaltung können sich unmittelbar an das SVN anschließen lassen.

Ergänzend zu den Möglichkeiten in § 15 Abs. 1 S. 2 SächsEGovG geht der Gesetzgeber in § 15 Abs. 1 S. 3 SächsEGovG davon aus, dass die Träger der Selbstverwaltung auch eine Schnittstelle benutzen können müssen, die einen Übergang an das SVN ermöglicht und die eine mit dem SVN vergleichbare Funktionalität und eine gleichwertige Informationssicherheit gewährleistet. Diese Norm zielt auf die Träger der öffentlichen Verwaltung ab, die bisher noch keinen gesicherten Zugang zum KDN haben.

Über die Ermächtigung in § 15 Abs. 2 SächsEGovG wird die Staatsregierung befugt, nähere Regelung durch Rechtsverordnung zu treffen, die ein Mindestsicherheitsniveau und Minimal-Leistungsmerkmale für diesen Übergang vorschreiben, soweit dies erforderlich sein sollte, um die Vergleichbarkeit in Sicherheit und Funktionalität mit dem SVN herzustellen.

Die Staatsregierung ist somit nicht verpflichtet, eine entsprechende Rechtsverordnung zu erlassen. Sofern die Schnittstelle existiert und dabei die Mindestanforderungen an den sicheren Datenaustausch im Sinne von § 15 Abs. 1 S. 3 SächsEGovG gewährleistet sind (wobei hierzu die in § 15 Abs. 2 S. 3, 4 SächsEGovG bestimmten Kriterien fachlich bei der Prüfung der Vergleichbarkeit heranzuziehen sind) und von den Nutzern eingehalten werden, reicht es aus, die Schnittstelle mit ihren Sicherheitsanforderungen in üblicher Weise z. B. durch Rundschreiben bekannt zu machen (siehe dazu zugleich Abschnitt B).

Soweit die Nutzung des Sächsischen Verwaltungsnetzes unter Informationssicherheitsgesichtspunkten nicht zwingend geboten erscheint, eröffnet zudem § 15 Abs. 1 S. 4 SächsEGovG eine Ausnahme von der allgemeinen Verpflichtung aus § 15 Abs. 1 S. 1 SächsEGovG. Dies ist insbesondere relevant für diejenigen Träger der Selbstverwaltung oder Beliehenen (auf die gemäß § 1 Abs. 1 S. 2 SächsEGovG diese Regelungen für die Träger der Selbstverwaltung Anwendung finden), die mit der staatlichen Verwaltungsebene nur sehr punktuell elektronisch kommunizieren. Für sie ist ein allgemein nutzbarer Netzzugang im Sinne von § 15 Abs. 1 S. 2, S. 3 SächsEGovG nicht notwendig, wenn in den Fachverfahren, über die die betroffenen Verwaltungseinheiten mit den staatlichen Behörden elektronisch kommunizieren, durch spezielle Rechtsvorschriften eine zuverlässige und sichere Datenübermittlung gewährleistet wird oder die Norm des § 15 Abs. 1 S. 4 SächsEGovG wegen der Besonderheiten des Fachverfahrens für nicht anwendbar bestimmt wird.

Derartige Regelungen finden sich schon jetzt in verschiedenen Rechtsverordnungen. So wird bundesrechtlich durch § 2 Abs. 2 S. 2, Abs. 3 S. 1, Abs. 4 S. 2 1. BMeldDÜV und durch § 6 Abs. 2a S. 4 2. BMeldDÜV normiert, dass die Meldebehörden die zwischen ihnen und die an Bundeseinrichtungen übermittelten Daten verschlüsseln und für die Datenübermittlung den Standard »OSCI-Transport« oder gemäß § 2 Abs. 3 S. 2 1. BMeldDÜV einen gleichwertigen Standard verwenden. Als gleichwertiger Standard gilt z. B. die Nutzung des OSCI-Gateways innerhalb des KDN und die Nutzung des InfoHighways Landesverwaltung Sachsen (jetzt: SVN) gemäß § 3 S. 1 und 5 Sächsische Meldeverordnung (SächsMeldVO). Vergleichbare Regelungen zum Standard »OSCI-Transport« sind z. B. auch in § 61c Abs. 3 S. 1, § 76a Abs. 1 S. 1 Aufenthaltsverordnung (AufenthV), § 6 Abs. 2, § 63 Abs. 2 S. 2 Personenstandsverordnung (PStV), § 8 Abs. 3 S. 1 Personalausweisverordnung (PAuswV), § 3 Abs. 3 S. 1 Passdatenerfassungs- und Übermittlungsverordnung (PassDEÜV) und § 2 Abs. 2 S. 4 Steueridentifikationsnummerverordnung (StIdV) enthalten. Die Verwendung alternativer Standards von entsprechendem Niveau oder mit Sicherheitseigenschaften von gleicher Qualität wird z. B. in § 76a Abs. 2 S. 2 AufenthV, § 63 Abs. 4 S. 1 PStV, § 8 Abs. 3 S. 4 und 5 sowie § 3 Abs. 3 S. 2 PassDEÜV (für WSDL / SOAP) vorgesehen.

Soweit solche fachverfahrensbezogenen Regelungen zum sicheren Datenaustausch vorliegen, ist es nicht zwingend notwendig, dass die Kommunikationswege zu den staatlichen Behörden über das SVN geführt werden. In diesen Fällen findet daher die in § 15 Abs. 1 S. 4 SächsEGovG enthaltene Ausnahme Anwendung.

B Empfehlungen zur Umsetzung

B.1 Zugang zum SVN über das KDN

Den kommunalen Trägern der Selbstverwaltung wird empfohlen, den Zugang zum Sächsischen Verwaltungsnetz (SVN) über das Kommunale Datennetz (KDN) herzustellen.

Die Träger der Selbstverwaltung haben im Zuge der Beantragung zur Nutzung der Schnittstelle gemäß § 15 Abs. 1 S. 3 SächsEGovG schriftlich zu erklären, dass sie die Anforderungen an den aktuellen Stand der Technik (z. B. für Virenscanner, Firewalls) einhalten.

B.2 Zugang zum SVN über eine Schnittstelle

Die Schnittstelle gemäß § 15 Abs. 1 S. 3 SächsEGovG umfasst den Netzübergang zum informationstechnischen Netz des Trägers der kommunalen Selbstverwaltung, den Netzübergang zum Sächsischen Verwaltungsnetz sowie die Datenverbindung zwischen beiden Netzübergängen. Dabei wird die Datenverbindung in der Regel über öffentliche Netze (Internet) realisiert. Eine vergleichbare Funktionalität und eine gleichwertige Informationssicherheit der Schnittstelle ist gegeben, wenn diese entsprechend den jeweils aktuellen IT-Grundschutz-Standards des BSI für die drei Grundwerte »Vertraulichkeit«, »Integrität« und »Verfügbarkeit« mindestens den Schutzbedarf »NORMAL« gewährleistet.

Sofern die Datenübermittlung dem Stand der Technik entsprechend verschlüsselt erfolgt, erfüllen folgende Verfahren diese Anforderungen:

Fachverfahren

Die Datenübermittlung erfolgt durch die Nutzung von Fachverfahren, die eine zuverlässige und sichere Datenübermittlung entsprechend dem Stand der Technik sicherstellen.

Die Freischaltung des Fachverfahrens kann bei der Leitstelle SVN beauftragt werden.

Die Anforderungen an die Art, die Mindest-Verfügbarkeit und die Mindest-Bandbreite der Datenverbindung sowie die Vorgaben zu den möglichen weiteren eingesetzten Protokollen (außer HTTPS) und zur verwendeten Systeminfrastruktur sind verfahrensspezifisch zu klären.

Speicherdienst

Die Übermittlung einzelner Dokumente erfolgt durch die Nutzung eines zuverlässigen und sicheren Speicherdienstes. Der Freistaat plant derzeit die Einrichtung eines besonders hoch gesicherten cloud-basierten Speicherdienstes innerhalb des SVN. Dieser wird voraussichtlich im Jahr 2016 zur Verfügung stehen. Die Daten im Speicherdienst werden verschlüsselt vorgehalten. Die zuverlässige und sichere Datenübermittlung erfolgt verschlüsselt entsprechend dem Stand der Technik.

Die Nutzung des Speicherdienstes als Schnittstelle nach § 15 Abs. 1 S. 3 SächsEGovG kann bei der Leitstelle SVN beauftragt werden.

E-Mail-Systeme

Zur gesicherten Kommunikation zwischen den Trägern der Selbstverwaltung und dem Freistaat Sachsen können die folgenden Kommunikationsmöglichkeiten genutzt werden:

- Secure Mail Gateway (SMGW) im SVN,
- Elektronisches Gerichts- und Verwaltungspostfach (EGVP),
- Governikus als Teilkomponente der Basiskomponente »Elektronische Signatur und Verschlüsselung« sowie
- De-Mail.

Die Übermittlung von E-Mails zwischen den E-Mail-Systemen der Träger der kommunalen Selbstverwaltung und den E-Mail-Systemen des Freistaates erfolgt generell verschlüsselt entsprechend dem Stand der Technik (Transportverschlüsselung).

Die Einhaltung des Standes der Technik wird durch die Leitstelle SVN bei allen drei genannten Verfahren der Datenübermittlung (Fachverfahren, Speicherdienst und E-Mail-Systeme) stichprobenartig geprüft. Bei erheblichen Mängeln kann die Datenübermittlung durch die Leitstelle SVN in Abstimmung mit dem Staatsministerium des Innern unterbunden werden.

C Beantwortung häufig gestellter Fragen

Frage 1: Welche Vorteile bringt der Anschluss an das KDN für meine Kommune?

> **Antwort**: Der entscheidende Vorteil für die Kommune besteht darin, dass gegenüber einem direkten Internetanschluss ein höheres Informationssicherheitsniveau garantiert wird.
> Das KDN ist als Intranet auf teilweise exklusiver Infrastruktur mit privatem Adressraum (gem. RFC 1597) realisiert. Datenpakete mit offiziellen Internetadressen werden nicht geroutet. Das KDN ist direkt mit dem Netz der Landesverwaltung (SVN), dem Internet und dem DOI-Netz (Verbindungsnetz des Bundes) über gesicherte Übergänge verbunden.
> Ein unerwünschter direkter Zugriff aus dem Internet auf interne Netze der angeschlossenen Verwaltungen ist nicht möglich. Dagegen können Diensteangebote der

angeschlossenen Teilnehmer im Internet oder selektiv im KDN / SVN bereitgestellt werden.
Integrierte Dienste, wie Realtime-Content-Scanning aller aufgerufenen Webseiten auf Schadcode, Virenscanning des gesamten Mailverkehrs oder eine sehr wirksame Anti-Spam-Lösung sowie ein zentrales Angriffserkennungssystem tragen wesentlich zur Informationssicherheit bei.
Nutzt eine angeschlossene Kommune das KDN-Mailrelay mit der Übertragungsoption STARTTSL (Standard bei aktuellen Mailservern) sind bereits die Mindestanforderungen des § 2 Abs. 1 SächsEGovG für die gesamte SVN/KDN-interne Mail-Kommunikation erfüllt. Für den Endnutzer ist dieser Verschlüsselungsmechanismus transparent – er muss nur einmalig die verschlüsselte Übertragung seines Mailclients zu seinem Mailserver aktivieren.

Frage 2: Wo finde ich Informationen und Ansprechpartner, wenn ein Anschluss an das KDN erwogen wird?

Antwort: Ansprechpartner für einen KDN-Anschluss ist die KDN GmbH. Zu den Möglichkeiten und Varianten eines Anschlusses berät auch die SAKD.

Frage 3: Was kostet ein Anschluss an das KDN?

Antwort: Jede Kommunalverwaltung hat Anspruch auf einen kostenfreien KDN-Basisanschluss. Die Kostenfreiheit umfasst alle Installations- und Betriebskosten.

Frage 4: Muss ich für einen Anschluss an das KDN Gesellschafter der KDN GmbH werden?

Antwort: Nein, die KDN GmbH schließt einen Vertrag mit der jeweiligen Kommune.

Frage 5: Welche Bandbreiten stellt das KDN für einen Anschluss zur Verfügung?

Antwort: Anschlussbandbreite und Serviceklasse sind technische Parameter des Basisanschlusses und richten sich nach der jeweiligen Größenklasse der Verwaltung. Darüber hinausgehende Bandbreiten oder andere Leistungen können hinzugebucht werden und sind kostenpflichtig. Die verfügbaren Anschlussvarianten sind auf der Website der KDN GmbH unter »Produkte« dargestellt.
Für die Aufrüstung des Basisanschlusses muss ein Angebot der KDN GmbH eingeholt werden. Dieses richtet sich nach einer vom KDN-Aufsichtsrat bestätigten Preisliste.

Frage 6: Wer kann mich dabei beraten, welchen Anschluss an das KDN ich für meine Verfahren benötige?

Antwort: Neben den genutzten Zentralverfahren mit der jeweiligen Anzahl simultaner Anwender richtet sich der Bandbreitenbedarf nach vielen weiten Bedingungen, wie

- Gesamtnutzerzahl in der Verwaltung und deren Internet-Nutzungsverhalten,
- Mailaufkommen in der Verwaltung,
- Bereitstellung eigener Dienste und Informationsangebote über den KDN-Anschluss sowie
- Anschluss von Telearbeitsplätzen über das KDN.

Die Kommunale Informationsverarbeitung Sachsen (KISA) bietet die meisten Zentralverfahren über das KDN an.

Die KDN GmbH überwacht die Auslastung der Kundenanschlüsse und ist gleichzeitig 100 prozentige Tochter der KISA, so dass hier die meisten Praxiserfahrungen zum benötigten Anschluss in Abhängigkeit von den Randbedingungen vorliegen.

Frage 7: Kann ich neben einem KDN-Anschluss weiter direkte Internetzugänge nutzen?

Antwort: Der Verzicht auf einen zusätzlichen Internetanschluss der Verwaltungen kann aus dem SächsEGovG nicht abgeleitet werden. Allerdings sind in diesem Fall zwei Bedingungen zu erfüllen:

1. Die gesamte E-Mail-Kommunikation der Maildomäne der Kommune muss über das KDN geführt werden (§ 2 Abs. 1 SächsEGovG).
2. Die Sicherheitsvorschriften der KDN GmbH für einen Zweitanschluss sind umzusetzen – inklusive Zertifizierung der Maßnahmen.

Frage 8: Muss ich bei einem KDN-Anschluss auch den DNS-Dienst für meine Domäne an die KDN GmbH übergeben?

Antwort: Nein, dazu besteht keine Verpflichtung, der DNS-Dienst könnte beim bisherigen Provider verbleiben. Allerdings empfiehlt sich eine Übergabe an die KDN GmbH, da Änderungen an der eigenen DNS-Zone, z. B. bei Mailumstellung auf das KDN, dann über das kostenfreie Change-Request-Verfahren des KDN, realisiert werden können.

Frage 9: Wo finde ich Informationen zu den IT-Grundschutz-Standards des BSI?

Antwort: Das BSI veröffentlicht Informationen zu den IT-Grundschutz-Standards auf der Webseiten des BSI zum Thema »IT-Grundschutz«.

§ 16 SächsEGovG – Elektronische Vorgangsbearbeitung und Aktenführung

§ 16 SächsEGovG lautet:

»Soweit die Träger der Selbstverwaltung sich für die elektronische Vorgangsbearbeitung oder Aktenführung entscheiden, gilt § 12 Abs. 1 Satz 2, Abs. 4 und 5 entsprechend.«

§ 12 Abs. 1 Satz 2 SächsEGovG lautet:

»Hierbei sind die Grundsätze ordnungsgemäßer Aktenführung und ordnungsmäßiger Aufbewahrung zu beachten.«

§ 12 Abs. 4 SächsEGovG lautet:

»In Papierform eingereichte Schriftstücke und sonstige Unterlagen sollen zur Ersetzung des Originals in ein elektronisches Dokument übertragen werden, soweit dies unter Beachtung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit den Grundsätzen ordnungsgemäßer Aktenführung und ordnungsmäßiger Aufbewahrung entspricht. Es ist sicherzustellen, dass die bildliche und inhaltliche Übereinstimmung mit dem Original besteht und nachvollzogen werden kann, wann und durch wen die Unterlagen übertragen wurden. Nach der Übertragung in elektronische Dokumente sollen die Originale, die nicht zurückgegeben wurden, vernichtet werden, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist.«

§ 12 Abs. 5 SächsEGovG lautet:

»Soweit es zur Erhaltung der Lesbarkeit erforderlich ist, können elektronisch gespeicherte Akten oder Aktenteile in ein anderes elektronisches Format überführt werden. Absatz 4 Satz 2 gilt entsprechend.«

A Erläuterung der Verpflichtung

Das SächsEGovG verpflichtet die Träger der Selbstverwaltung nicht dazu, die elektronische Vorgangsbearbeitung und Aktenführung einzuführen. § 16 SächsEGovG erklärt nur für den Fall, dass ein Träger der Selbstverwaltung sich für die elektronische Vorgangsbearbeitung oder Aktenführung entscheidet, die Regelungen des § 12 Abs. 1 S. 2, Abs. 4 und 5 SächsEGovG für entsprechend anwendbar. Die Norm gilt für die Träger der Selbstverwaltung seit dem 9. August 2014 (zum Begriff »Träger der Selbstverwaltung« siehe Erläuterungen zu § 2 Abs. 1 SächsEGovG). Entscheidet man sich für diese elektronische Aufgabenerfüllung sind nach § 12 Abs. 1 S. 2 SächsEGovG auch die Träger der Selbstverwaltung verpflichtet, die Grundsätze ordnungsgemäßer Aktenführung und ordnungsmäßiger Aufbewahrung zu beachten. Insoweit bestätigt die Regelung lediglich klarstellend die verfassungsrechtlichen Vorgaben für eine rechtmäßige Verwaltungsorganisation.

Zudem gelten die Vorschriften aus § 12 Abs. 4, 5 SächsEGovG zum ersetzenden Scannen von Papierdokumenten und zur lesbarkeitserhaltenden Umformatierung elektronischer Dokumente auch für die Träger der Selbstverwaltung.

Der Verweis durch § 16 SächsEGovG auf die Regelung in § 12 Abs. 4 SächsEGovG enthält mit den dort vorgesehenen Soll-Pflichten zum ersetzenden Scannen - für diejenigen kommunalen Träger der Selbstverwaltung, die sich für die elektronische Vorgangsbearbeitung oder Aktenführung entschieden haben - einen Eingriff in ihre verfassungsrechtlich garantierte

Organisationshoheit. Denn mit der Einführung der elektronischen Vorgangsbearbeitung oder Aktenführung ist auch die Digitalisierung der eingereichten Dokumente eine Pflicht. Allerdings sind diese »Soll-Pflichten« durch die Grundsätze der Wirtschaftlichkeit und Sparsamkeit sowie die Grundsätze der ordnungsgemäßen Aktenführung und Aufbewahrung begrenzt, da diese uneingeschränkt auch für Träger der Selbstverwaltung gelten. Diese Soll-Pflichten enthalten zudem keine näheren Vorgaben zur Art und Weise der elektronischen Vorgangsbearbeitung oder Aktenführung und belassen den Kommunen bei ihrer Umsetzung ausreichend regionale Spielräume. Durch die Regelung der Zulässigkeit des ersetzenden Scannens wird die Rechtssicherheit für die Mitarbeiter bei der konkreten Verwaltungstätigkeit erhöht und hierdurch ein Anreiz zur Einführung der elektronischen Vorgangsbearbeitung und Aktenführung geschaffen. Erst diese verwaltungsinterne Umstrukturierung in den Behörden und Einrichtungen der Träger der Selbstverwaltung wird es erlauben, den mit der elektronischen Außenkommunikation begonnenen Wechsel in den Verwaltungsprozessen medienbruchfrei für ganze Verwaltungsverfahren zu vervollständigen und somit in signifikantem Ausmaß von den durch die IT-Unterstützung ermöglichten Erleichterungen und Beschleunigungen in den Verwaltungsabläufen zu profitieren.

Der Verweis durch § 16 SächsEGovG auf die Regelung in § 12 Abs. 5 SächsEGovG eröffnet für die Träger der Selbstverwaltung lediglich eine zusätzliche rechtliche Möglichkeit, auch von der zur lesbarkeitserhaltenden Umformatierung elektronischer Dokumente Gebrauch zu machen.

B Empfehlungen zur Umsetzung

Die Empfehlungen zur Umsetzung des § 16 SächsEGovG beschränken sich an dieser Stelle ausschließlich auf die Grundsätze ordnungsgemäßer Aktenführung und ordnungsmäßiger Aufbewahrung (siehe Abschnitt B.1), des ersetzenden Scannens (siehe Abschnitt B.2) sowie die Umformatierung elektronischer Dokumente (siehe Abschnitt B.4). Nur diese Regelungen des SächsEGovG sind von den Trägern der Selbstverwaltung zu beachten. Weitergehende Hinweise zur Einführung der elektronischen Vorgangsbearbeitung oder Aktenführung enthält der Handlungsleitfaden zur Umsetzung des SächsEGovG in staatlichen Behörden (siehe Empfehlungen zur Umsetzung des § 12 SächsEGovG).

B.1 Ordnungsgemäße Aktenführung und Aufbewahrung

Werden Vorgänge elektronisch bearbeitet oder Akten elektronisch geführt, müssen bei Verwendung elektronischer Akten - ebenso wie bei Papierakten - die Grundsätze ordnungsgemäßer Aktenführung beachtet werden. Die elektronischen Akten müssen daher ebenso den Geboten der Vollständigkeit, der Aktenstabilität und der Nachvollziehbarkeit genügen sowie wahrheitsgemäß geführt werden. Dies bestätigt § 12 Abs. 1 S. 2 SächsEGovG ausdrücklich, ebenso wie die Notwendigkeit, die Grundsätze ordnungsmäßiger Aufbewahrung zu beachten. Die Formulierung ist angelehnt an § 110a SGB IV. Elektronische Akten müssen demnach während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sein und lesbar gemacht werden können. Des Weiteren ist im Hinblick auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme - ein dem Stand der Technik entsprechender Schutz vor Veränderung, Fälschung und Einsichtnahme durch Unbefugte - zu gewähren.

B.2 Ersetzendes Scannen

Vom ersetzenden Scannen spricht man dann, wenn das Papieroriginal nach dem Abschluss des Scanvorganges (Umwandlung in ein elektronisches Abbild) zurückgegeben oder vernichtet wird.

§ 12 Abs. 4 SächsEGovG enthält die Regelung zur Überführung von Papierdokumenten in die elektronische Form durch Scannen. Ohne eine solche Möglichkeit können elektronische Akten nicht vollständig im Sinne von § 12 Abs. 1 S. 2 SächsEGovG geführt werden.

Nach § 12 Abs. 4 S. 1 SächsEGovG sollen dabei die in Papierform eingereichten Dokumente in der Regel in ein elektronisches Dokument übertragen werden. Das Gesetz selbst gibt dafür keinen Standard vor und verlangt auch nicht die Einhaltung eines solchen Standards (anders § 7 Abs. 1 S. 2 E-Government-Gesetz des Bundes, das hier den Stand der Technik vorschreibt).

Der Grundsatz der Aktenwahrheit und -klarheit und die Anforderungen an die Nachvollziehbarkeit und Nachweisbarkeit behördlichen Handelns verlangen aber eine Umwandlung von Papierdokumenten in elektronische Dokumente durch Scannen, die zumindest dem Stand der Technik entsprechen müssen oder mit einem solchen Standard vergleichbar sind. Anderenfalls ist die Beweiskraft der eingescannten Dokumente vor Gericht geschwächt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierfür die Technische Richtlinie »Rechtssicheres Scannen« (TR RESISCAN) erarbeitet, deren Anwendung zur Erfüllung des Standes der Technik empfohlen wird. Die TR RESISCAN enthält technische, organisatorische und personelle Anforderungen, um ein rechtssicheres Scannen zu ermöglichen. Die vom Gesetz geforderte Sicherstellung der bildlichen und inhaltlichen Übereinstimmung zwischen beiden Dokumentformen erfordert keine vollständige Sichtprüfung aller erstellten digitalen Dokumente.

Auch in der Praxis eingeführte und automatisierte und wenn möglich zertifizierte Scanverfahren, die dem Stand der Technik entsprechen, können verwendet werden, wenn die Stichproben keine Defizite feststellen. Auch geringfügige technisch bedingte Abweichungen in Größe und Farbe können hingenommen werden, soweit die beweisrelevanten Inhalte des Originals nicht beeinträchtigt sind. Da es auf den Beweiswert von Größen und Farben in Dokumenten ankommt, ist dies durch die eingesetzte Technik (z. B. bei Speicherplatz, Bandbreite, Einsatz von Farbscannern) abzusichern. Durch geeignete technische Maßnahmen muss zudem sichergestellt sein, dass man nachvollziehen kann, welcher Mitarbeiter wann die Übertragung durchgeführt hat. Hier kommen primär z. B. elektronische Zeitstempelinformationen auf dem Scanprodukt oder auch Informationen in den Metadaten des elektronischen Dokuments in Betracht. Die nach § 371b ZPO für die Beweiskraft gescannter öffentlicher Urkunden (Urkundsbeweis) notwendige Bestätigung, dass das elektronische Dokument mit der Urschrift bildlich und inhaltlich übereinstimmt (stellt quasi einen elektronischen Beglaubigungsvermerk dar) muss ebenfalls mit dem Scanprodukt verbunden sein.

Die jeweilige aktenführende Stelle kann und sollte auch konkretisierende organisatorische Regelungen in einer internen Organisationsverfügung (Scan-Anweisung) treffen. Da die vollständige elektronische Akte allein maßgebend ist, sollen eingegangene Papierdokumente gemäß § 12 Abs. 4 S. 3 SächsEGovG nach dem Scannen grundsätzlich zurückgegeben oder vernichtet werden. Eine vorübergehende Aufbewahrung der Papierdokumente nach dem Scanvorgang kann für eine Qualitätsprüfung zweckmäßig sein. Dabei dürfte in der Praxis - je nach konkreter organisatorischer Ausgestaltung - eine Frist zwischen drei Wochen und drei Monaten ausreichend sein. Hierdurch können nachträgliche Korrekturen vorgenommen werden, falls trotz der technischen und organisatorischen Vorkehrungen für die

Ausgestaltung eines sicheren Scanvorganges ein Dokument fehlerhaft oder unvollständig eingescannt worden sein sollte.

Ausnahmen von der grundsätzlichen Vernichtung des Papierdokumentes

Eine ausnahmslose Vernichtung des Papieroriginals durch die Behörde ist aufgrund des Rechts auf effektiven Rechtsschutz nach Art. 19 Abs. 4 GG und Art. 38 SächsVerf sowie aufgrund des im Rechtsstaatsprinzip verbürgten Justizgewährungsanspruches nicht möglich. Hierdurch wird dem Einzelnen gegenüber dem Gesetzgeber ein Anspruch auf effektiven Rechtsschutz, d. h. auf eine tatsächlich wirksame und möglichst lückenlose gerichtliche Kontrolle vermittelt. Dies beinhaltet im Falle eines Rechtsstreits eine vollständige Prüfung des Streitbegehrens in rechtlicher und tatsächlicher Hinsicht. Materiell-rechtliche und prozessuale gesetzliche Regelungen dürfen den Anspruch des Einzelnen auf eine tatsächlich wirksame gerichtliche Kontrolle nicht in unzumutbarer, aus Sachgründen nicht mehr zu rechtfertigender Weise erschweren.

Eine solche Erschwerung der wirksamen gerichtlichen Kontrolle träte jedoch ein, wenn beweisrelevante, in Papierform eingereichte Dokumente nach dem Scannen ausnahmslos vernichtet würden. Die mit der Vernichtung solcher Dokumente verbundene Verschlechterung der Beweisführungsmöglichkeiten kann durch das Einscannen nicht kompensiert werden. Gescannte Dokumente werden - wenn sie nicht den Anforderungen des § 371b ZPO an öffentliche Urkunden entsprechen oder wenn es sich um Scans von Privaturkunden handelt im Regelfall, anders als das Original, nicht im Urkundsbeweis eingeführt, sondern sind Gegenstand des Augenscheins. Sie können nicht mehr ausreichend auf die Unversehrtheit der Urkunde, die Echtheit der Unterschrift, den Zeitpunkt ihrer Entstehung und nachfolgende Veränderungen geprüft werden. Da dieser Beweisnachteil nicht ausgeglichen und auch nicht sachlich gerechtfertigt werden kann, müssen beweisrelevante Originalunterlagen zurückgegeben oder aufbewahrt werden, wobei hier auch die Interessen möglicher Drittbetroffener in mehrpoligen Rechtsverhältnissen angemessen zu berücksichtigen sind. Im Falle eines Rechtsstreits wäre das Gericht durch die Vernichtung des Dokuments gehindert, sich anhand des Originals eine eigene Auffassung von dessen Beweiskraft und dem zu beurteilenden Sachverhalt zu machen. Faktisch würde das Gericht an das behördliche Beweisergebnis gebunden. Der durch Art. 19 Abs. 4 GG garantierte Rechtsweg zu den Gerichten beinhaltet jedoch die Kompetenz der Gerichte, die Verwaltung in der Gesetzesauslegung, der Tatsachenfeststellung und der Gesetzesanwendung zu korrigieren. Eine Bindung an administrative Tatsachenfeststellungen oder Wertungen ist damit unvereinbar.

Daher gelten Ausnahmen von der grundsätzlichen Vernichtung des Papierdokumentes gemäß § 12 Abs. 4 S. 3 SächsEGovG, wenn es für das Verfahren auf die Originaleigenschaft des Papierdokumentes ankommt – oder wenn eine Vernichtung aus anderen Gründen ausgeschlossen ist. Als solche Ausnahmetatbestände kommen neben dem Ausschluss der Vernichtung durch eine spezialgesetzliche Vorschrift einerseits die Überlassung der Dokumente an die Behörde nur für die Dauer der Bearbeitung und andererseits das Bestehen eines Beweisführungsrechtes eines Verfahrensbeteiligten an den Urkunden in Betracht. Im Falle der nur vorübergehenden Überlassung geht das Eigentum an den Urkunden nicht auf die Behörde über, die daher dem Absender − nach ausdrücklicher Erklärung oder wenn sich dies aus den Umständen ergibt − zurückzugeben sind (z. B. einerseits: Rückgabe von vorgelegten Heirats- oder Geburtsurkunden nach Prüfung und Scannen aber andererseits: Einscannen und Vernichten einer Meldebescheinigung, die zur Vorlage bei der Behörde bestimmt ist). Zur Vermeidung von Unsicherheiten in der alltäglichen Praxis sollten die Behörden in einer Organisationsverfügung (Scan-Anweisung) klarstellende Einzelheiten hierzu festlegen und für die betroffenen Mitarbeiter insoweit Rechtssicherheit schaffen. Hier kann auch geregelt werden, dass wirklich wichtige Urkunden

auch im Original weiter verwahrt werden (z. B. Ausfertigungen von Gesetzen; Staatsverträge; beamtenrechtliche Ernennungsurkunden; die nur handschriftlich unterschrieben wirksamen Bürgschaftsurkunden gemäß § 766 BGB).

Fiktion des Urkundsbeweis bei eingescannten öffentlichen Urkunden nach § 371b ZPO

Bisher enthalten § 55b Abs. 5 VwGO, § 110d SGB IV sowie § 110b Abs. 3 OWiG Erleichterungen im Umgang mit eingescannten Dokumenten jeweils für die Bereiche der Verwaltungsgerichtsbarkeit, der Sozialversicherung sowie für die Verfahren bei Ordnungswidrigkeiten. Das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (ERVG) sieht für alle gerichtlichen Verfahren (außer für die Strafverfahren und für die Grundbuch- und Registerverfahren) Beweiserleichterungen für bestimmte De-Mail-Nachrichten und für nach dem Stand der Technik gescannte öffentliche Urkunden vor. Auf die gescannten öffentlichen Urkunden finden danach seit dem 17. Oktober 2013 die allgemeinen und speziellen Beweiskraftregeln für öffentliche Urkunden aus §§ 165, 314, 415, 417 und 418 ZPO Anwendung und bei Vorliegen einer qualifizierten elektronischen Signatur auch die Echtheitsvermutung aus § 437 Abs. 1 ZPO. Beim korrekten Einscannen öffentlicher Urkunden entstehen dann beweiswerterhaltende elektronische Dokumente, die gegenüber der Papierurkunde keinem Beweisverlust unterliegen (vgl. weiterführend den Aufsatz »Beweisführung mittels ersetzend gescannter Dokumente« von Rossnagel / Nebel in NJW 13/2014, S. 886-891, in dem in 14 simulierten Gerichtsverfahren vor Zivil- und Finanzgerichten die Beweiskraft des papierersetzenden Scannens vor Gericht untersucht wurde).

B.3 Digitalisierung von Papierschriftgut

Eingehendes Papierschriftgut soll in die elektronische Form überführt werden, um eine vollständige elektronische Akte zu erstellen. Auch wenn kein ersetzendes Scannen entsprechend § 12 Abs. 4 SächsEGovG zulässigerweise durchgeführt wird und damit das eingegangene Papierschriftgut in der Behörde parallel aufbewahrt werden muss, sollte eine Digitalisierung für die elektronische Akte durchgeführt werden. Damit wird eine vollständige Bearbeitung der Akteninhalte innerhalb der Behörde mit Hilfe der elektronischen Akte ermöglicht.

Es wird empfohlen das Papierschriftgut im Ergebnis der Digitalisierung in ein PDF-Format mit Texterkennung (OCR) zu überführen.

Papierschriftgut, das einer Behörde übergeben wird, aber nicht aktenrelevant ist, muss im Rahmen des § 12 Abs. 4 SächsEGovG nicht digitalisiert werden.

Wenn Papierschriftgut zusätzlich zur digitalen Form oder nur in Papier vorhanden ist, so ist dies in den Registraturdaten der elektronischen Akte zu vermerken. In diesen Daten sollte auch der jeweils aktuelle Standort der Aufbewahrung des Papierschriftgutes geeignet (z. B. konkreter Regal- oder Kistenstandort) vermerkt werden.

Für die Digitalisierung von Papierschriftgut ist die einzusetzende Scan-Infrastruktur so zu dimensionieren, dass das üblicherweise eingehende Papierschriftgut unverzüglich in die elektronische Form überführt und registriert werden kann (z. B. muss der durchschnittliche Umfang von 100 Posteingängen á 5 Seiten innerhalb von 3 Arbeitsstunden gescannt werden können).

Papierschriftgut in Sonderformaten (z. B. Formate größer DIN A3) oder Papierschriftgut auf besonders dünnem oder extrem starkem Papier braucht im Regelfall nicht digitalisiert zu werden. Diese Formen treten so selten auf, dass es in diesen Fällen nicht den Grundsätzen von Wirtschaftlichkeit und Sparsamkeit entspricht, hierfür eine besondere technische Scan-Infrastruktur vorzuhalten.

Durch die Behörde sind Arbeitsanweisungen zu erstellen, aus denen hervorgeht,

- welches Papierschriftgut zu digitalisieren ist,
- welches davon in der Behörde aufzubewahren ist und
- welches im Rahmen des ersetzenden Scannens nach der Frist für die Durchführung einer Qualitätssicherung des Scan-Ergebnisses vernichtet oder an den Absender zurückgegeben wird.

Wird die Digitalisierung von Papierschriftgut durch Dritte (andere Behörden oder externe Dienstleister) durchgeführt, so muss dies bei der organisatorischen Ausgestaltung des Scan-Prozesses beachtet werden. Die Behörden haben in diesen Fällen für die Umsetzung der Scan-Arbeiten die Dritten auf das Datengeheimnis nach § 6 SächsDSG zu verpflichten, eine Verpflichtung nach BDSG ist nicht ausreichend. Eine schriftliche Vereinbarung zur Datenverarbeitung im Auftrag entsprechend § 7 SächsDSG ist in jeden Fall erforderlich. Auch muss der für die Übertragung der gescannten Dokumente oder Inhalte genutzte Kommunikationskanal dem Schutzbedarf des digitalisierten Papierschriftgutes entsprechen.

Der § 16 i. V. m. § 12 Abs. 4 SächsEGovG erlaubt den Trägern der Selbstverwaltung, ein ersetzendes Scannen durchzuführen. Ergänzend muss dazu der bei der Behörde etablierte Scan-Prozess aus organisatorischer und technischer Sicht dokumentiert werden. Aus Sicht des SMI wird die Anwendung der Technischen Richtlinie des BSI zum ersetzenden Scannen (BSI TR 03138 RESISCAN) empfohlen.

Entsprechend der TR RESISCAN ist auf Basis einer Schutzbedarfsanalyse für das zu scannende Papierschriftgut der Scan-Prozess auszugestalten und eine Verfahrensanweisung für das Scannen (Scan-Anweisung) zu erstellen. Bestandteil dieser Verfahrensanweisung sollten auch die o. g. Arbeitsanweisungen sein.

Das Vorgehen nach TR RESISCAN beinhaltet ferner die Durchführung einer Risikoanalyse. Entsprechend dem Ergebnis der Risikoanalyse sind die Häufigkeit und der Umfang der durchzuführenden Stichproben zur Überprüfung der bildlichen und inhaltlichen Übereinstimmung zwischen Original und Scanergebnis zu definieren. Ergeben sich aus diesen Stichprobenprüfungen Qualitätsmängel beim Scannen, so sind die aufgetretenen Fehler oder Qualitätsmängel zu analysieren. Der Scan-Prozess ist entsprechend anzupassen, beziehungsweise die zum Einsatz kommende Scan-Technik ist zu optimieren. Außerdem kann eine temporäre oder dauerhafte Änderung der Stichprobenhäufigkeit notwendig sein.

B.4 Lesbarkeitserhaltende Umformatierung elektronischer Dokumente

Der Verweis durch § 16 SächsEGovG auf die Regelung in § 12 Abs. 5 SächsEGovG eröffnet für die Träger der Selbstverwaltung die Möglichkeit, von der lesbarkeitserhaltenden Umformatierung elektronischer Dokumente Gebrauch zu machen. Die Regelung in § 12 Abs. 5 SächsEGovG gibt den Behörden dazu die Rechtsgrundlage. Dabei ist darauf zu achten, dass die Beweiskraft der Dokumente erhalten bleibt. Insofern ist der Umwandlungsprozess ebenfalls nach Maßgabe einer Organisationsanweisung durchzuführen und zu dokumentieren.

Aus den Grundsätzen der ordnungsgemäßen Aktenführung ergibt sich, dass Schriftgut während der gesamten Aufbewahrungszeit in der Behörde nutzbar und lesbar sein muss. Dieser Grundsatz gilt unabhängig von dem für die Aktenführung eingesetzten Medium und damit auch für Schriftgut in der elektronischen Akte.

Bei elektronischen Daten kann nicht bei allen Dateiformaten sichergestellt werden, dass eine Nutzung über Jahre möglich ist. So können beispielsweise zum Einsatz kommende Programme für die Anzeige der elektronischen Daten die ursprünglich verwendeten Dateiformate nicht mehr unterstützen oder die bisher genutzten Anzeigeprogramme unter neueren Betriebssystemen nicht mehr verfügbar sein. Diese Probleme treten insbesondere bei nicht offengelegten und proprietären Dateiformaten auf.

Um die Nutzbarkeit und Lesbarkeit der elektronischen Daten zu erhalten, ist daher – sofern nicht schon früher nötig – spätestens beim Abschluss der aktiven Bearbeitung der elektronischen Akte (z. B. Abschlussverfügung) eine Formatkonvertierung in langzeitfähige Dateiformate zu prüfen und ggf. durchzuführen. Für dokumentenbasiertes Schriftgut ist dies derzeit das Format PDF/A (ISO-Standard 19005). Für strukturierte Daten kann XML eingesetzt werden. Für andere Formate (z. B. Video- oder Musikdateien) kann in Abstimmung mit dem Sächsischen Staatsarchiv ein geeignetes langzeitfähiges Dateiformat festgelegt werden. Bei längeren Aufbewahrungsfristen und der fortschreitenden technischen Entwicklung kann es sein, dass ein ursprünglich genutztes Langzeitformat durch ein anderes ersetzt werden soll oder muss. In diesen Fall ist eine erneute Konvertierung in das dann aktuelle Langzeitformat vorzunehmen. Für die Durchführung von Konvertierungen wird eine Konvertierungsplattform als verfahrensunabhängiger zentral betriebener Dienst konzipiert.

Schwerpunkt der Konvertierung ist der Erhalt der Lesbarkeit. Sofern es auf die Bearbeitungs- und Darstellungsoptionen des ursprünglichen Originalformats ankommt, kann parallel zum langzeitfähigen Format auch das Originalformat aufbewahrt werden.

C Beantwortung häufig gestellter Fragen

Frage 1: Welche Anforderungen bestehen an ein rechtssicheres ersetzendes Scannen?

> **Antwort**: Ein rechtssicheres ersetzendes Scannen verlangt, sicherzustellen, dass die bildliche und inhaltliche Übereinstimmung mit dem Original besteht. Auf die Ausführungen im Abschnitt B.2 wird verwiesen.

Frage 2: Welche Empfehlungen gibt es für Behörden, die bereits vor Inkrafttreten des SächsEGovG mit der elektronischen Aktenführung begonnen haben?

> **Antwort**: Soweit bereits vor Inkrafttreten des SächsEGovG begonnen wurde auf eine generelle elektronische Aktenführung umzustellen, ist die weitere Umsetzung so zu gestalten, dass sie die Anforderungen des § 12 Abs. 1 S. 2 SächsEGovG erfüllt, ohne dass parallel eine vollständige Papierakte geführt werden muss. Sämtliche rechtliche Folgen, z. B. Einsichtsrechte, knüpfen sodann folgerichtig an die elektronische Akte an.

§ 19 Abs. 3 SächsEGovG – Sorbische Sprache

§ 19 Abs. 3 SächsEGovG lautet:

»Unberührt bleiben die Regelungen nach § 9 des Gesetzes über die Rechte der Sorben im Freistaat Sachsen (Sächsisches Sorbengesetz – SächsSorbG) vom 31. März 1999 (SächsGVBl. S. 161), das zuletzt durch Artikel 59a des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130, 141) geändert worden ist, in der jeweils geltenden Fassung. Die notwendigen Voraussetzungen zur Verwendung der sorbischen Sprache sind zu schaffen.«

A Erläuterung der Verpflichtung

Inkrafttreten der Verpflichtung

Die Verpflichtung aus § 19 Abs. 3 S. 1 SächsEGovG, die notwendigen, im wesentlichen technischen Voraussetzungen zur Verwendung der sorbischen Sprache zu schaffen, um Bürgern im sorbischen Siedlungsgebiet die elektronische Kommunikation mit staatlichen Behörden und Trägern der Selbstverwaltung (vgl. Ausführungen zu §§ 1, 2 Abs. 1 SächsEGovG) in sorbischer Sprache zu ermöglichen, ist unmittelbar nach Verkündung des SächsEGovG in Kraft getreten. Sie gilt seit dem 9. August 2014.

Sofern jedoch bereits zuvor, seit Inkrafttreten des SächsSorbG im Jahre 1999, z. B. der Zugang für elektronische Dokumente (in sorbischer Sprache) im Rahmen der Verwaltungsverfahren (nach VwVfG, SGB I oder AO) eröffnet wurde, musste diese Vorschrift bereits zum Zeitpunkt der Zugangseröffnung inhaltlich erfüllt sein.

Adressat der Verpflichtung

Soweit der Anwendungsbereich des SächsEGovG eröffnet ist (vgl. § 1 SächsEGovG), sind die Adressaten der Verpflichtung alle Behörden des Freistaates Sachsen und die seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, die ihren Sitz im sorbischen Siedlungsgebiet haben. Dies gilt ebenfalls für die Gerichtsverwaltungen in den Landkreisen Bautzen und Görlitz (§ 19 Abs. 3 S. 1 SächsEGovG, § 1 Abs. 3 SächsEGovG i. V. m. § 9 Abs. 2 S. 2 SächsSorbG). D. h. § 19 Abs. 3 S. 1 SächsEGovG gilt beispielsweise nicht für die Gerichte selbst oder den MDR, da diese vom Anwendungsbereich des Gesetzes von vornherein ausgenommen sind. Insofern sind von der Verpflichtung aus § 19 Abs. 3 S. 2 SächsEGovG nicht alle der in § 9 SächsSorbG genannten öffentlichen Stellen / Gerichte umfasst. Das sorbische Siedlungsgebiet ist in § 3 SächsSorbG definiert und durch die Anlage zum SächsSorbG abgegrenzt.

Mittelbar umfasst sind aber auch bestimmte Staatsbehörden, die ihren Sitz außerhalb des sorbischen Siedlungsgebietes haben, aber Aufgaben erfüllen, die sie für die Behörden im Siedlungsgebiet (mit) erledigen. Ansonsten würde die Vorschrift erkennbar leerlaufen. So betrifft dies z. B. das Sächsische Staatsministerium des Innern oder die Sächsische Staatskanzlei in ihrer Zuständigkeit für den Betrieb und die Weiterentwicklung der Basiskomponenten und moderner Bürgerdienste, die zentral aus Dresden für alle Staatsbehörden bereit gestellt werden und den Kommunen zur Mitnutzung (im vertraglichen Umfang) bereit stehen.

Inhalt der Verpflichtung

Die Verpflichtung liegt darin, die im Wesentlichen technischen Voraussetzungen zur Verwendung der sorbischen Sprache zu schaffen. Damit müssen alle informationstechnischen

Systeme von den Staatsbehörden und Trägern der Selbstverwaltung, die für einen Empfang oder eine Übermittlung von Nachrichten in sorbischer Sprache eingesetzt oder vorgehalten werden, so ertüchtigt werden, dass Bürger im sorbischen Siedlungsgebiet ihre Anliegen auch auf elektronischem Wege vor Behörden in sorbischer Sprache vorbringen können und dass ihnen – sofern dies nach § 9 SächsSorbG erfolgen soll – auch entsprechend geantwortet werden kann. Im Gebiet des Freistaates Sachsen handelt es sich um die Sprache Obersorbisch.

Dies bedeutet, dass die direkte Kommunikation in sorbischer Sprache grundsätzlich in beide Richtungen ermöglicht werden muss. Stellt eine Behörde z. B. Formulare zum Ausfüllen bereit, die elektronisch automatisiert weiterverarbeitet werden, müssen diese auch in sorbischer Sprache ausfüllbar und bearbeitbar sein. Die elektronische Rückantwort der Behörde an den Betroffenen auf einen in dieser Weise z.B. elektronisch gestellten Antrag kann, muss aber nicht in Sorbisch erfolgen. Hier hat die Behörde vielmehr das Recht zu entscheiden, ob sie die Antwort (den Bescheid) in deutscher oder in sorbischer Sprache sendet (vgl. § 9 Abs. 1 S. 3 SächsSorbG).

Da mit einem Teil der Basiskomponenten (vgl. zum Begriff der Basiskomponenten die Definition in § 10 Abs. 1 S. 1 SächsEGovG) die Möglichkeit besteht, mit staatlichen oder kommunalen Behörden in Kontakt zu treten, muss auch hier dem gesetzlichen Anspruch genüge getan werden. Vorrangig zu betrachten sind die Basiskomponenten Beteiligungsplattform, Zuständigkeitsfinder, Formularservice und Antragsmanagement.

B Empfehlungen zur Umsetzung

Um den Einsatz der sorbischen Sprache informationstechnologisch zu ermöglichen, müssen die IT-Systeme den Unicode-Standard und damit die UTF-8 Kodierung unterstützen und sollten internationalisierbar (für Mehrsprachigkeit vorbereitet) sein. Mit UTF-8 lassen sich alle Zeichen des sorbischen Alphabets darstellen (und darüber hinaus alle Zeichen slawischer Sprachen).

Aus Gründen der Interoperabilität sollten daher alle IT-Systeme durchgängig auf UTF-8 basieren. Bei der Beauftragung und Abnahme neuer Systemkomponenten ist die Einhaltung dieses Kriteriums festzuschreiben und zu kontrollieren. Bei bereits bestehenden Komponenten ist zu prüfen, ob sie UTF-8-basiert sind. Ist dies nicht der Fall, ist die Anpassung zu beauftragen.

Besonders im Bereich der Datenbank-Technologien ist darauf zu achten, dass Daten im UTF-8-Format gespeichert werden. Ist ein System nach heutigem Stand der Technik internationalisierbar, so ist es auch für die sorbische Sprache vorbereitet und kann im Bedarfsfall dahingehend ohne programmiertechnischen Aufwand angepasst werden.

Bei Spracheinstellungen (Lokalisierungsinformationen) sind die Konventionen für die sorbische Sprache (Datum etc.) des Unicode-Konsortiums, verfügbar im Common Local Data Repository (CLDR) zu beachten.

C Beantwortung häufig gestellter Fragen

Frage 1: Entstehen durch die Schaffung der technischen Voraussetzungen zur Verwendung der sorbischen Sprache besondere finanzielle Aufwände?

> **Antwort**: Aufwände entstehen dort, wo ältere Anwendungen auf UTF-8 umgestellt werden müssen. Da UTF-8 bereits seit Jahren dem aktuellen Standard entspricht, ist bei Neubeauftragungen das Augenmerk auf die Verwendung von UTF-8 zu richten sowie im Bedarfsfall die Unterstützung der Mehrsprachigkeit vorzusehen.

Frage 2: Müssen die Backend-Nutzerinterfaces von E-Government-Anwendungen für Mehrsprachigkeit ausgelegt sein?

> **Antwort**: Ja, denn die jeweiligen Backend-Nutzerinterfaces der Anwendungen müssen im Bedarfsfall ins Sorbische übertragen werden können.

Frage 3: Wie verhält sich die Festlegung auf die Zeichensatzkodierung UTF-8 zur Entscheidung 2014/04 des IT-Planungsrates »Einheitlicher Zeichensatz für Datenübermittlung und Registerführung«?

> **Antwort**: Die in dieser Entscheidung des IT-Planungsrats als verbindlich festgelegte Untermenge des Unicode-Zeichensatzes enthält auch die sorbischen Sonderzeichen. Dieser Standard »Lateinische Zeichen in Unicode« legt die Menge der zulässigen Zeichen mit ihren Unicode-Codepoints fest; er trifft jedoch keine über Unicode hinausgehenden Aussagen über die Transformation in Bytefolgen. Die Kodierung per UTF-8 wird also nicht explizit vorgeschrieben, im Anhang der Entscheidung 2014/04 des IT-Planungsrates ist aber unter »Encoding« die Kodierung UTF-8 als die übliche und am weitesten verbreitete Kodierung benannt.

Frage 4: Inwiefern unterstützen die Office-Anwendungen die sorbische Sprache?

> **Antwort**: Microsoft Office unterstützt derzeit die sorbische Sprache nur unvollständig. Zwar können z. B. in Microsoft Word Texte in der Spracheinstellung als ober- bzw. niedersorbisch markiert werden. Allerdings stellt Microsoft kein Modul für die Rechtschreibprüfung zur Verfügung.
> Demgegenüber stellen OpenOffice und LibreOffice auch in den offiziellen Distributionen oder über das offizielle Verzeichnis für Erweiterungen eine Rechtschreibprüfung bereit (siehe Beispiel für obersorbische Rechtschreibprüfung in OpenOffice).

Frage 5: Müssen auch die technischen Voraussetzungen für einen barrierefreien Zugang in sorbischer Sprache geschaffen werden?

> **Antwort**: Ja, soweit der Anwendungsbereich des § 9 Abs. 1 SächsSorbG eröffnet ist bzw. reicht. Sollte der Zugang zu den Anwendungen (Portale, Frontend- oder Backend-Nutzerinterfaces) barrierefrei sein (vgl. dazu § 7 SächsEGovG), so sollte auch die sorbische Sprache berücksichtigt werden. Voraussetzung für die Berücksichtigung der sorbischen Sprache ist jedoch die Verfügbarkeit einer entsprechenden Text2Speech-Software.

FAQ-Liste

FAQs zu § 1 SächsEGovG – Anwendungsbereich:

Frage 1: Richtet sich die Verschlüsselung bei der Übermittlung von Passbildern zwischen Pass- und Ordnungsbehörde in Bußgeldverfahren nach dem Sächsischen E-Government-Gesetz oder nach dem Passgesetz des Bundes und welches Verschlüsselungsniveau gilt hier?

Frage 2: Sowohl § 7 SächsEGovG als auch § 7 SächsIntegrG enthalten Regeln über die Barrierefreiheit. Verdrängt das SächsEGovG als das zeitlich später erlassene Gesetz das SächsIntegrG?

Frage 3: Unter den Voraussetzungen des § 4 SächsEGovG ist es beispielsweise möglich, kommunale Satzungen einer Gemeinde auch oder sogar ausschließlich elektronisch zu verkünden. Widerspricht dies nicht § 2 der Kommunalbekanntmachungsverordnung (KomBekVO), die für öffentliche Bekanntmachungen von Satzungen nur den Abdruck (also eine Papierfassung), z. B. im Amtsblatt der Gemeinde oder des Landkreises, dem die Gemeinde angehört, vorschreibt?

FAQs zu § 2 Abs. 1 SächsEGovG – Elektronische Kommunikation und Verschlüsselungsverfahren:

Frage 1: Fordert das SächsEGovG eine Inhalts- oder eine Transportverschlüsselung?

Frage 2: § 2 Abs. 1 S. 3 SächsEGovG erlaubt begrenzte Ausnahmen von der Anwendung der Verschlüsselung bei der elektronischen Kommunikation. Ist bei Datenübermittlungen zwischen Trägern der Selbstverwaltung untereinander und mit anderen Behörden, die ans SVN / KDN angeschlossen sind, insbesondere für den E-Mail-Verkehr, eine Verschlüsselung notwendig oder sind die Netze sicher genug, dass die Datenübermittlungen wie bisher unverschlüsselt erfolgen können?

Frage 3: Ändert sich daran etwas, wenn personenbezogene Daten (z. B. Passbilder zwischen Passbehörde und Polizeidienststelle) übermittelt werden?

Frage 4: Wie sind Frage 2 und Frage 3 zu beantworten, wenn die Datenübermittlung innerhalb einer Kommune (z. B. zwischen Ordnungsamt und Meldebehörde) a) im Intranet erfolgt oder b) über das Internet abgewickelt wird (insb. wenn die Behörden in unterschiedlichen Orts- oder Stadtteilen oder Gemeinden ihren Dienstort haben)?

Frage 5: Welche Verschlüsselungsverfahren, die auch vom Bürger unkompliziert eingesetzt werden können, sind zu empfehlen?

Frage 6: Was ist der Unterschied zwischen öffentlichem und privatem Schlüssel (Zertifikat)?

Frage 7: Wie kann ein externer Kommunikationspartner seinen Schlüssel der Behörde bekannt machen?

Frage 8: Wie kann eine Behörde ihren Schlüssel dem externen Kommunikationspartner bekannt machen?

Frage 9: Können Behörden verschlüsselte Nachrichten nur an Empfänger senden, von denen der Behörde bereits ein Empfängerschlüssel bekannt ist?

Frage 10: Kann die Behörde vorab ermitteln, ob für den Empfänger bereits ein Schlüssel bekannt ist?

Frage 11: Welche E-Mail-Adresse (Domain-Teil) bekommt der Antragsteller als passiver oder aktiver Nutzer des SMGW?

Frage 12: Was geschieht mit der Original-E-Mail, die im SMGW entschlüsselt und geprüft wurde? Ist diese für den Empfänger der Nachricht noch von Bedeutung?

Frage 13: Wie kann eine E-Mail Ende-zu-Ende verschlüsselt werden?

Frage 14: Was ist bei der Auswahl eines Zertifikatsanbieters (Certificate Authority, CA) zu beachten?

Frage 15: Unter welchen Voraussetzungen kann ein Serverzertifikat der Sachsen Global CA beantragt werden?

Frage 16: Stellt die Sachsen Global CA Wildcard-Zertifikate für die SSL-Verschlüsselung aller Server oder Webanwendungen einer Domäne aus?

Frage 17: Welche Zertifikatsprofile sind in der Sachsen Global CA implementiert?

Frage 18: Unter welchen Voraussetzungen kann ein Nutzerzertifikat der Sachsen Global CA beantragt werden?

Frage 19: Was kostet ein Zertifikat?

Frage 20: Was ist bei der Beantragung von Zertifikaten für Umlautdomains bei der Sachsen Global CA zu beachten?

Frage 21: Welche Client-Zertifikate können für OSCI (EGVP) eingesetzt werden?

FAQs zu § 2 Abs. 2 SächsEGovG – Zugangseröffnung für Dokumente mit qeS:

Frage 1: Können die im Rahmen der Umsetzung der EU-Dienstleistungsrichtlinie eingerichteten technischen Verfahren zur Signaturprüfung auch für andere Verwaltungsverfahren eingesetzt werden?

Frage 2: Wie ist mit Dokumenten umzugehen, die mit einer ausländischen Signatur versehen sind?

Frage 3: Wann gilt eine Signatur als geprüft mit positivem Ergebnis. Kann es z. B. auch ein positives Prüfergebnis geben, wenn ein Dritter das einzureichende Dokument signiert hat?

Frage 4: Wie ist praktisch mit qeS-signierten und geprüften Dateien in der weiteren Aktendokumentation (DMS, VBS) umzugehen, um auch langfristig die erfolgreiche Signaturprüfung zu dokumentieren?

Frage 5: Wie muss mit einem Dokument umgegangen werden, das zwar mit einer qeS signiert wurde, für das aber die Schriftform überhaupt nicht erforderlich ist?

FAQs zu § 3 SächsEGovG – Elektronische Zahlungsverfahren:

Frage 1: Warum sollte ich die Basiskomponente Zahlungsverkehr (ePayBL®) einsetzen und nicht einfach ein kommerzielles Tool (z. B. PayPal®)?

Frage 2: Was muss ich tun, um mir einen Überblick über Details und weitere Dokumente von ePayBL® zu verschaffen?

Frage 3: Welche Haushaltssysteme werden von ePayBL® bereits unterstützt?

Frage 4: Wie hoch ist der Aufwand für den Einsatz von ePayBL®?

FAQs zu § 5 Abs. 1 SächsEGovG – Datenschutz- und Informationssicherheitskonzepte:

Frage 1: Wann sollten der zuständige Datenschutzbeauftragte und der Informationssicherheitsbeauftragte in ein E-Government-Projekt einbezogenen werden?

Frage 2: Muss der behördliche Datenschutzbeauftragte das Datenschutzkonzept selbst erstellen?

Frage 3: Müssen ein Informationssicherheitskonzept und daneben ein Datenschutzkonzept erstellt werden?

Frage 4: Zu welchen Schutzzielen der Informationssicherheit und des Datenschutzrechts müssen technische und organisatorische Maßnahmen geprüft und festgelegt werden?

Frage 5: Besteht die Verpflichtung für staatliche Behörden und Träger der Selbstverwaltung, Datenschutz- und Informationssicherheitskonzepte zu erstellen und zu pflegen, auch für bereits im Einsatz befindliche »Altverfahren«, mit denen personenbezogene Daten verarbeitet werden?

Frage 6: Welche Informationsmaterialien können für die Beantwortung von Datenschutzfragen im Zusammenhang mit der Erstellung von Datenschutzkonzepten neben den bereits im Textteil genannten Orientierungshilfen noch herangezogen werden?

FAQs zu § 7 SächsEGovG – Barrierefreiheit:

Frage 1: Wo kann ich das im SächsEGovG genannte Sächsische Integrationsgesetz einsehen?

Frage 2: Wo erhalte ich konkrete Hinweise zur barrierefreien Gestaltung elektronischer Kommunikation und elektronischer Dokumente?

Frage 3: An wen wende ich mich, wenn ich feststelle, dass bei einer der eingebundenen Basiskomponenten Barrieren für Menschen mit Behinderungen bestehen?

Frage 4: Welche gesetzlichen Grundlagen gelten für Internetseiten und Internetangebote in Form von elektronischen Formularen, Vordrucken und Dokumenten?

Frage 5: In welchem Zeitraum müssen Internetangebote an die Anforderungen der Barrierefreiheit angepasst werden?

Frage 6: Für welche Gruppen von Menschen mit Behinderungen sind typischerweise Vorkehrungen zu treffen, damit ein barrierefreier Zugang und eine barrierefreie Nutzung elektronischer Kommunikation möglich sind?

Frage 7: In welchem Umfang sind Vorkehrungen zu treffen?

Frage 8: Hat ein behinderter Mitarbeiter eines Landratsamtes bei Durchführung eines Verwaltungsverfahrens mit einer Gemeinde aus §§ 7, 2 Abs. 1 i. V. m. § 1 Abs. 1

SächsEGovG einen Anspruch darauf, dass ihr der entsprechend zuständige Mitarbeiter der Gemeindeverwaltung beispielsweise eine dafür notwendige E-Mail barrierefrei zusendet?

Frage 9: Wie ist Frage 8 zu beantworten, wenn die Behörden die elektronische Vorgangsbearbeitung und Aktenführung eingeführt haben?

Frage 10: Wie kann ich sicherstellen, dass meine Internetangebote barrierefrei sind?

FAQs zu § 13 Abs. 1 SächsEGovG – Informationssicherheit:

Frage 1: Gibt es zeitliche Fristen für die Umsetzung der Vorgaben nach § 13 Abs. 1 i. V. m. § 9 Abs. 2 SächsEGovG?

FAQs zu § 15 SächsEGovG – Datenübermittlung:

Frage 1: Welche Vorteile bringt der Anschluss an das KDN für meine Kommune?

Frage 2: Wo finde ich Informationen und Ansprechpartner, wenn ein Anschluss an das KDN erwogen wird?

Frage 3: Was kostet ein Anschluss an das KDN?

Frage 4: Muss ich für einen Anschluss an das KDN Gesellschafter der KDN GmbH werden?

Frage 5: Welche Bandbreiten stellt das KDN für einen Anschluss zur Verfügung?

Frage 6: Wer kann mich dabei beraten, welchen Anschluss an das KDN ich für meine Verfahren benötige?

Frage 7: Kann ich neben einem KDN-Anschluss weiter direkte Internetzugänge nutzen?

Frage 8: Muss ich bei einem KDN-Anschluss auch den DNS-Dienst für meine Domäne an die KDN GmbH übergeben?

Frage 9: Wo finde ich Informationen zu den IT-Grundschutz-Standards des BSI?

FAQs zu § 16 SächsEGovG – Informationssicherheit:

Frage 1: Welche Anforderungen bestehen an ein rechtssicheres ersetzendes Scannen?

Frage 2: Welche Empfehlungen gibt es für Behörden, die bereits vor Inkrafttreten des SächsEGovG mit der elektronischen Aktenführung begonnen haben?

FAQs zu § 19 Abs. 3 SächsEGovG – Sorbische Sprache:

Frage 1: Entstehen durch die Schaffung der technischen Voraussetzungen zur Verwendung der sorbischen Sprache besondere finanzielle Aufwände?

Frage 2: Müssen die Backend-Nutzerinterfaces von E-Government-Anwendungen für Mehrsprachigkeit ausgelegt sein?

Frage 3: Wie verhält sich die Festlegung auf die Zeichensatzkodierung UTF-8 zur Entscheidung 2014/04 des IT-Planungsrates »Einheitlicher Zeichensatz für Datenübermittlung und Registerführung«?

Frage 4: Inwiefern unterstützen die Office-Anwendungen die sorbische Sprache?

Frage 5: Müssen auch die technischen Voraussetzungen für einen barrierefreien Zugang in sorbischer Sprache geschaffen werden?

Anhang

Liste der an der Erarbeitung des Handlungsleitfadens Beteiligten

Name	*Organisationseinheit*
§ 1 SächsEGovG – Anwendungsbereich Sämtliche Abschnitte A (Erläuterungen der Verpflichtungen) des Handlungsleitfadens	
Herr Rech, Burghard	SMI
§ 2 Abs. 1 SächsEGovG – Elektronische Kommunikation und Verschlüsselungsverfahren	
Herr Schenkel, Robert	SID
Herr Apolle, Haiko	LK Bautzen
Frau Burkhardt, Sandra	Stadt Leipzig
Herr Eichinger, Heiko	LK Mittelsachsen
Herr Kresse, Joachim	LK Meißen
Herr Meier, Hans-Jürgen	Landeshauptstadt Dresden
Herr Nikol, Uwe	SAKD
Herr Oßwald, Mario	SächsDSB
Herr Uhlig, Frank	KISA
Herr Wollschläger, Holger	Lecos GmbH
§ 2 Abs. 2 SächsEGovG – Zugangseröffnung für Dokumente mit qeS	
Herr Walther, Karl-Heinz	SMI
Herr Apolle, Haiko	LK Bautzen
Frau Burkhardt, Sandra	Stadt Leipzig
Frau Herold, Christin	KISA
Herr Höller, Friedemann	Landeshauptstadt Dresden
Herr Kirsten, Thomas	LK Sächs. Schweiz-Osterzgebirge
Herr Konzelmann, Lars	SDB
Herr Kresse, Joachim	LK Meißen
Herr Pohle, Horst	SAKD
Herr Schenkel, Robert	SID
Herr Wollschläger, Holger	Lecos GmbH
§ 3 SächsEGovG – Elektronische Zahlungen	
Herr Kaiser, Uwe	SID
Herr Aurig, Thilo	SMF
Herr Lehnert, Uwe	SAKD
Frau Mannewitz, Juliane	SMF
…	LV komm. Kassenverwaltung

Name	*Organisationseinheit*
§ 5 Abs. 1 SächsEGovG – Datenschutz- und Informationssicherheitskonzepte	
Frau Lotze-Kaufhold, Caterina	SMI
Herr Damm, Christoph	SMI
Frau Krombholz, Sabine	SMI
Herr Schramm, Tino	SAKD
Frau Thalheim-Heinecke, Katja	SDB
…	DSB der Ressorts
§ 7 SächsEGovG – Barrierefreiheit	
Frau Flume, Christina	SMI
Herr Prof. Dr. Kahlisch, Thomas	DZB
Herr Kosel, Bolko	Stadt Leipzig
Herr Kretschmer, Jürgen	SAKD
Frau Dr. Schwerdel-Schmidt, Heike	SK
Herr Vogel, Dirk	KISA
Herr Welsch, Michael	SMS
§ 13 Abs. 1 SächsEGovG – Informationssicherheit	
Herr Damm, Christoph	SMI
Herr Anker, Rico	LK Meißen
Herr Hoppenz, Uwe	SID
Frau Körner, Kerstin	LK Sächs. Schweiz-Osterzgebirge
Herr Meier, Hans-Jürgen	Landeshauptstadt Dresden
Herr Nikol, Uwe	SAKD
Herr Oßwald, Mario	SDB
Herr Schultz, Thomas	Stadt Leipzig
…	BfIS der Ressorts
§ 15 SächsEGovG – Datenübermittlung	
Herr Benkendorff, Dirk	SMI
Herr Fahland, Andreas	SMI
Herr Söhnel, Andreas	SID
§ 16 SächsEGovG – Elektronische Vorgangsbearbeitung und Aktenführung	
Herr Feske, Nicol	SMI
…	Ressort-Ansprechpartner (AG eVA.SAX)
§ 19 Abs. 3 SächsEGovG – Sorbische Sprache	
Frau Dr. Schwerdel-Schmidt	SK
Herr Baier, Bernhard	SID
Herr Kowar, Marko	Domowina – Bund Lausitzer Sorben e.V.
Herr Böhmak, Wito	Freier IT-Berater / Domowina

Name	*Organisationseinheit*
Kernteam	
Frau Dr. Höhne, Gudrun	SMI
Herr Popp, Ronald	SMI
Herr Rech, Burghard	SMI
Herr Dr. Naumann, Tino	SDB
Herr Weber, Thomas	SAKD
Herr Piskol, Daniel	SSG
Frau Sommerfeld, Yvonne	SLKT
Frau Lotze-Kaufhold, Caterina	SMI
Frau Flume, Christina	SMI
Herr Damm, Christoph	SMI
Herr Feske, Nicol	SMI
Herr Walther, Karl-Heinz	SMI
Herr Gattwinkel, Dietmar	SID
Herr Kaiser, Uwe	SID
Herr Schenkel, Robert	SID
Frau Hoffmann, Mary Ann	Syncwork AG
Herr Dr. Sachs, Hans-Martin	Syncwork AG

Im Handlungsleitfaden verwendete Abkürzungen

Abkürzung	*Erläuterung*
BaK	Basiskomponente
BfIS	Beauftragte für Informationssicherheit
BfO	Beauftragte für Organisation
CA	Certificate Authority
CMS	Content Management System
DFN	Deutsches Forschungsnetz
DENIC	Deutsches Network Information Center
DMS	Dokumenten-Managementsystem
DNS	Domain Name Service
DSB	Datenschutzbeauftragter
DZB	Deutsche Zentralbücherei für Blinde
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
FAQ	Frequently Asked Questions
HLF	Handlungsleitfaden
HTTPS	HyperText Transfer Protocol Secure
InterNIC	Internet Network Information Center
ITEG	Informationstechnik und E-Government
KDN	Kommunales Datennetz
KISA	Zweckverband Kommunale Informationsverarbeitung Sachsen
LK	Landkreis
LV	Landesverband
OCR	Optical Character Recognition
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
qeS	Qualifizierte elektronische Signatur
SGCA	Sachsen Global Certificate Authority
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung
SDB	Sächsischer Datenschutzbeauftragter
SID	Staatsbetrieb Sächsische Informatik Dienste
SK	Sächsische Staatskanzlei
SLKT	Sächsischer Landkreistag
SLT	Sächsischer Landtag
SMF	Sächsisches Staatsministerium der Finanzen
SMGW	Secure Mail Gateway
SMI	Sächsisches Staatsministerium des Innern
SMS	Sächsisches Staatsministerium für Soziales und Verbraucherschutz
SOAP	Simple Object Access Protocol

Abkürzung	*Erläuterung*
SSG	Sächsischer Städte- und Gemeindetag
SSL	Secure Sockets Layer
StaLa	Statistisches Landesamt
SVN	Sächsisches Verwaltungsnetz
S/MIME	Secure / Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
VBS	Vorgangsbearbeitungssystem
VwV	Verwaltungsvorschrift
WSDL	Web Services Description Language
XÖV	XML in der Öffentlichen Verwaltung

Anlagen

Textfassung SächsEGovG (Artikel 1) in:

- Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen und zur Änderung des Gesetzes über die Errichtung der SAKD

Anlagen zu § 2 Abs. 2 SächsEGovG – Zugangseröffnung für Dokumente mit qualifiziert elektronischer Signatur:

- §2(2)_Zugangseröffnung.pdf
- §2(2)_Workshop_AK-ITEG_Zugang_für_signierte_Dokumente.pdf
- §2(2)_Elektronische_Signaturen_LRA-Bautzen.pdf

Anlagen zu § 5 Abs. 1 SächsEGovG – Datenschutz- und Informationssicherheitskonzepte:

- §5(1)_Checkliste_DS-IS-Konzepte.pdf
- §5(1)_Rollenkonzept_Basiskomponenten.pdf

Anlagen zu § 7 SächsEGovG – Barrierefreiheit:

- §7_Anforderungen_an_die_Barrierefreiheit_von_PDF-Dokumenten.pdf

Anlagen zu § 13 Abs. 1 SächsEGovG – Informationssicherheit:

- §9(2)+§13(1)_Beantragung_Serverzertifikate_Apache.pdf
- §9(2)+§13(1)_Beantragung_Serverzertifikate_Microsoft_IIS.pdf
- §9(2)+§13(1)_Einschaltung_Outlook-Verschlüsselung.pdf
- §9(2)+§13(1)_Handlungsempfehlungen_Verschlüsselung.pdf
- §9(2)+§13(1)_Beschluss_Optimierung_HTTPS-Konfiguration.pdf
- §9(2)+§13(1)_Optimierung_HTTPS-Konfiguration_Apache.pdf
- §9(2)+§13(1)_Optimierung_HTTPS-Konfiguration_Microsoft_IIS.pdf

Impressum

Herausgeber:
Sächsisches Staatsministerium des Innern (SMI), Abteilung 6
Wilhelm-Buck-Straße 4, 01097 Dresden

Redaktion:
Interministerielle Arbeitsgruppe aus Vertretern staatlicher und kommunaler Behörden
SMI, Referat 61, egov-itgrundsatz-gremien@smi.sachsen.de
Syncwork AG, Dresden

Redaktionsschluss:
19. Dezember 2014