Rechtskonform in 16 Schritten

Schritt-für-Schritt-Anleitung zur schnellen Umsetzung des E-Government-Gesetzes in kommunalen Behörden

Version: 1.2

Status: Freigabe

Herausgeber:

Sächsische Anstalt für kommunale Datenverarbeitung
Bischofstraße 18
01877 Bischofswerda

Telefon: 03594 77 52-0
Telefax: 03594 77 52-99
E-Mail: **sakd@sakd.de**
Internet: **www.sakd.de**

Inhalt

A. Einleitung

Diese Anleitung richtet sich an Verantwortliche und Mitarbeiter in sächsischen Kommunalverwaltungen, die aktiv am Prozess der Umsetzung des SächsEGovG beteiligt und dafür verantwortlich sind, die Verwaltung schnell rechtskonform zu machen.

Die Ausführungen fassen die obligatorischen Umsetzungserfordernisse in einer maximal komprimierten Schritt-für-Schritt-Anleitung zusammen.

Hintergründe, Erläuterungen zu einzelnen Verpflichtungen, erweiterte Umsetzungsempfehlungen und –alternativen sowie Antworten auf häufig auftretende Fragen zum SächsEGovG sind in einem umfangreichen „Handlungsleitfaden zur Umsetzung in kommunalen Behörden“, herausgegeben durch das Sächsische Staatsministerium der Justiz und für Europa, enthalten, der an dieser Stelle erwähnt und ausdrücklich zur ergänzenden Lektüre empfohlen wird.

Über die hier beschriebenen Schritte hinaus sind in den Verwaltungen auch organisatorische Regelungen zu treffen bzw. anzupassen (z. B. geänderte oder erweiterte Zuständigkeiten, Umgang mit ggf. fehlerhaft signierten E-Mail-Eingängen, notwendige Erweiterung der Schriftgutordnungen etc.). Diese unterscheiden sich je nach konkreter Aufbauorganisation der Verwaltungen. Sie sind gemeinsam mit den für Organisation Zuständigen zu erarbeiten und von der Leitung umzusetzen.

Im Zusammenhang mit dem SächsEGovG geänderte Aufgabenzuschnitte ziehen Schulungs- und Qualifizierungsbedarf für die betroffenen Mitarbeiter nach sich (z. B. bei der Durchführung von Signaturprüfungen oder hinsichtlich Datenschutz und Informationssicherheit).

Erst die Summe von sowohl technischen als auch organisatorischen und personellen Maßnahmen wird dazu führen, das SächsEGovG rechtssicher, aufwandsarm und zielführend im Sinne der elektronischen Verwaltungstätigkeit umzusetzen.

Die Mitarbeiter der SAKD stehen Ihnen auf diesem Weg beratend und unterstützend zur Seite.

B. Umsetzungspflichten mit Fristsetzung

§ 2 Abs. 1 – Elektronische Kommunikation grundsätzlich mit Verschlüsselung ermöglichen

§ 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.«

Umsetzungspflicht: alle Kommunalverwaltungen **ab 09.08.2014**

Arbeitsschritte:

1. Festlegung der Empfangs-E-Mail-Adresse, z. B. poststelle@gemeinde-xy.de

2. Verschlüsselte KDN-interne E-Mail-Kommunikation einstellen
   a) Aktivierung der Verschlüsselung zwischen Mailserver und KDN-Mailrelais
      siehe http://www.sakd.de/sakd_newsletterbei-traege.html?&tx_ttnews%5Btt_news%5D=658&cHash=3c23d845c84d36ddfd3f1cd0ea21352a

   b) Aktivierung der Verschlüsselung zwischen Mailclient und Mailserver (abhängig vom verwendeten Mailclient)

3. Verschlüsselte Kommunikation mit Bürgern bzw. Unternehmen ermöglichen
   a) Verschlüsselungszertifikat für die gem. Pkt.1 festgelegte E-Mail-Adresse beantragen, z. B. beim SID:
      - Sachsen Global CA kostenfreies Gruppenzertifikat beantragen (siehe Anlage 1 „Beantragung: Sachsen Global CA Gruppenzertifikat)

      Beispiele für alternative kostenpflichtige Anbieter:
      - Sparkassenverlag
        https://www.s-trust.de/service_support/email_zert/infocenter/index.htm
      - Bundesdruckerei
        https://www.bundesdruckerei.de/de/2752-d-trust-ssl

   b) Zertifikat / Gruppenzertifikat an dem Arbeitsplatz, der die eingehenden E-Mails empfängt, installieren

   c) Öffentlichen Schlüssel, Empfangs-E-Mail-Adresse, max. Mail-Größe und zugelassene Dateiformate auf der Internetseite publizieren
      z. B. http://www.landkreis-mittelsachsen.de/buergerservice/fachbereiche/5398.html

4. Erstellung bzw. Überarbeitung von organisatorischen Regelungen z. B. hinsichtlich:
   - Zuständigkeit für die Empfangs-E-Mail-Adresse
   - Weiterleitung eingehender Nachrichten
   - Anpassung Registratur- und Schriftgutordnung

§ 2 Abs. 2 – Zugangseröffnung für (verschlüsselte) Dokumente mit qualifiziert elektronischer Signatur

§ 2 Abs. 2 Satz 1 SächsEGovG lautet:

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

Umsetzungspflicht: alle Kommunalverwaltungen **ab 01.09.2016**

Kommunalverwaltungen, die Bundesrecht ausführen **ab 01.07.2014**

Arbeitsschritte:

1. Festlegung der Empfangs-E-Mail-Adresse, z. B. poststelle@gemeinde-xy.de

   Für signierte Zugänge möglichst die gleiche Empfangs-E-Mail-Adresse verwenden, wie für verschlüsselte Eingänge.

2. Empfangs-E-Mail-Adresse, technische Rahmenbedingungen (akzeptierte Dateiformate, max. Mailgröße, Festlegungen zum Signaturstandard z.B. PKCS#7) auf der Internetseite der Verwaltung publizieren.

3. Arbeitsplatz, der den Posteingang auf der in Pkt. 1 festgelegten E-Mail-Adresse bearbeitet, mit Signaturprüfungskomponente ausstatten:
   - Governikus Signer (manuelle Prüfung)
     Beantragung zur kostenlosen Bereitstellung der Software Governikus Signer unter:
     https://fs.egov.sachsen.de/formserv/findform?shortname=smjusv3_esv_govern&formtecid=2&areashortname=SMJus_RV3_ESV
   - Einweisung bzw. Schulung der mit der Aufgabe betrauten Mitarbeiter im Umgang mit der Software Governikus Signer.
   - Festlegungen zum Umgang bei nicht signierten oder fehlerhaft signierten Eingängen oder Nichteinhaltung der unter Pkt. 2 getroffenen Festlegungen vornehmen (Absender informieren,…)

4. Signaturprüfung mit Governikus Signer vornehmen und Prüfprotokoll in geschützter Umgebung, z. B. in einem DMS oder in einem durch Zugriffsrechte gesicherten Dateisystem abspeichern.

§ 3 – Elektronische Zahlungen ermöglichen

§ 3 SächsEGovG lautet:

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

Umsetzungspflicht: alle Kommunalverwaltungen **ab 09.08.2014**

Anforderung:

Es muss mindestens eine elektronische Zahlungsmöglichkeit angeboten werden.

Diese allgemeine Pflicht ist schon erfüllt, wenn z. B. die Überweisung als ein auch elektronisch nutzbares Zahlungsverfahren angeboten wird.

Arbeitsschritte:

1. Prüfung, ob Bezahlvorgänge existieren, die entsprechend geltender Vorschriften (Dienstanweisungen, Satzungen, etc.) nur per Barzahlung abgewickelt werden dürfen.

2. Anpassung dieser Vorschriften entsprechend § 3 SächsEGovG.

3. Einsatz elektronischer Zahlungsmöglichkeiten prüfen und ggfs. realisieren.

Weitere Zahlungsmöglichkeiten (erweiterte Umsetzung):

Nutzung der Basiskomponente Zahlungsverkehr (BaK ZV) der E-Government-Plattform des Freistaates Sachsen mit den Zahlungsmöglichkeiten:

- Vorkasse / auf Rechnung
- Lastschrift (SEPA-Lastschrift)
- Giropay ®
- Kreditkarte

Für die Behörden im Freistaat Sachsen und die sächsischen Kommunen ist der Einsatz der BaK ZV kostenfrei. Es entstehen (geringe) Transaktionskosten pro Buchung.

§ 5 Abs. 1 – 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.«

Umsetzungspflicht: alle Kommunalverwaltungen **ab 09.08.2014**

§ 5 Abs. 1 SächsEGovG verpflichtet 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.

Der eingangs erwähnte „Handlungsleitfaden zur Umsetzung in kommunalen Behörden“ enthält sehr ausführliche Erklärungen zur Erstellung der Konzepte. Als Instrument dafür wurde im Rahmen der Erstellung des Handlungsleitfadens die „Checkliste zur Erstellung von Datenschutz- und Informationssicherheitskonzepten“ (siehe Anlage 2) erarbeitet.

§ 7 – Barrierefreiheit elektronische Kommunikation und elektronische Dokumente

§ 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.«

Umsetzungspflicht: alle Kommunalverwaltungen **ab 09.08.2014**

Als „Elektronische Kommunikation und elektronische Dokumente“ sind zum Beispiel E-Mail-Verkehr, Internetangebote, Dokumente und Antragsformulare zu verstehen.

Maßgebliche Anforderungen an Barrierefreiheit in diesem Zusammenhang sind in der BITV 2.0 (Barrierefreie-Informations-Technik-Verordnung des Bundes) und dem Standard PDF/UA (Portable Document Format / Universal Accessibility) benannt.

Arbeitsschritte:

1. Organisatorische Sicherstellung der barrierefreien Gestaltung nach den maßgeblichen Anforderungen für zukünftige elektronische Kommunikation und elektronische Dokumente

2. Erstellung und Umsetzung eines Konzeptes zur schrittweisen barrierefreien Umgestaltung nach den maßgeblichen Anforderungen für bestehende elektronische Kommunikation und elektronische Dokumente mit definierten Zeitpunkten

3. Prüfung der Erfüllung der Anforderungen der Punkte 1. und 2.

Dienstleister zur Erstellung und Zertifizierung barrierefreier Webseiten enthält Anlage 3.

§ 13 Abs. 1 – Informationssicherheit

§ 13 Abs. 1 SächsEGovG lautet:

»Für die am E-Government beteiligten Träger der Selbstverwaltung gilt § 9 Abs. 2 Satz 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.«

Umsetzungspflicht: alle Kommunalverwaltungen **ab 09.08.2014**

Arbeitsschritte:

1. Leitlinie zur Informationssicherheit erarbeiten und umsetzen
   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.

2. Informationssicherheitskonzept(e) erstellen und umsetzen entsprechend der „Checkliste zur Erstellung von Datenschutz- und Informationssicherheitskonzepten“ des Sächsischen Datenschutzbeauftragten (siehe Anlage 2).

§ 15 Abs. 1 – Datenübermittlung (verwaltungsübergreifende elektronische 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 Satz 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.«

Umsetzungspflicht: alle Kommunalverwaltungen **ab 09.08.2014**

Arbeitsschritte:

1. Zugang zum Sächsischen Verwaltungsnetz (SVN) über das kommunale Datennetz (KDN) beantragen www.kdn-gmbh.de.

2. Einrichtung eines kostenfreien KDN-Basisanschlusses

Achtung! Die in § 15 Abs. 2 angeführte Rechtsverordnung existiert noch nicht, so dass derzeit nur durch einen KDN-Anschluss Rechtssicherheit gewährleistet werden kann.

C. Umsetzungspflichten ohne Fristsetzung

§ 24 Abs. 2 i. V. m. § 10 Abs. 3: Datenlieferung für Zuständigkeitsfinder

Eine Konkretisierung der Verpflichtung erfolgt mit Erlass einer entsprechenden Rechtsverordnung zu den E-Government-Basiskomponenten.

§§ 13 Abs. 2 i. V. m. § 15 Abs. 3: Durchleitungsnormen für Beschlüsse des IT-Planungsrates

Die Norm verpflichtet die Träger der Selbstverwaltung zur Umsetzung der vom IT-Planungsrat gefassten Beschlüsse nach deren Veröffentlichung.

D. Anlage 1: Beantragung eines Sachsen Global CA Gruppenzertifikats

Die Nutzungsbedingungen der Sachsen Global CA sind beschrieben unter https://info.pca.dfn.de/sachsen-global-ca/cpcps-1.1.pdf.

Bitte beachten Sie, dass die Abholung Ihres Zertifikates vom gleichen Rechner und im gleichen Browser erfolgen sollte, der bei der Beantragung verwendet wurde.

Zur kostenfreien Erstellung eines Gruppenzertifikats bitte gehen Sie auf folgende Seite: https://pki.pca.dfn.de/sachsen-global-ca/pub.

Es erfolgt eine automatische Weiterleitung auf die zentrale Zertifikatsantragsseite der neuen "Sachsen Global CA". Dort im Reiter "Zertifikate" den Menüpunkt "Nutzerzertifikat" wählen.

Tragen Sie in die Antragsmaske die Daten unter Beachtung folgender Punkte ein:

E-Mail: des Verantwortlichen für das Zertifikat -> Empfänger der Zertifikatsdatei

Name: Dem Behördennamen **zwingend Präfix „GRP:“** voranstellen! Gegebenenfalls ein Verfahrenszusatz separiert durch „-„ angeben, zum Beispiel: „GRP: Musterstadt“ oder „GRP: Musterstadt– OSCI XYZ“

Abteilung: Behördenname + gegebenenfalls Bereich, z. B. „Musterstadt – EDV“
Sie müssen der Zertifizierungsrichtlinie zustimmen. Die Checkbox zur Veröffentlichung des Zertifikates sollten Sie nicht aktivieren.

Weitere Hinweise finden Sie unter http://www.pki.dfn.de/index.php?id=faqpkiallgemein.

Drucken und unterschreiben Sie den Antrag bzw. lassen Sie den Antrag unterschreiben. Senden Sie den ausgedruckten, unterschriebenen Zertifikatsantrag an:

Antragsadresse:

Staatsbetrieb Sächsische Informatik Dienste
Fachbereich 3.1 | E-Government- und Querschnittverfahren
Zertifikatsmanager SachsenGlobalCA
Riesaer Str. 7 | 01129 Dresden

Um die Bearbeitungszeit (Postlaufzeit) zu verkürzen, wird vorab ein FAX des Antrages akzeptiert. Senden Sie dieses an: (03 57 8) 33 55 47 91. Sobald der unterschriebene Antrag der Registrierungsstelle vorliegt, wird er kurzfristig geprüft und freigegeben. Nach Freigabe bekommen Sie eine E-Mail von pki@smi.sachsen.de mit Auslieferung des Zertifikats.

Für Rückfragen steht Ihnen ein E-Mail-Support unter SachsenGlobalCaZm@sid.sachsen.de zur Verfügung.

E. Anlage 2: Checkliste zur Erstellung von Datenschutz- und Informationssicherheitskonzepten

1. Verantwortlichkeiten im Datenschutz festlegen

Organisatorische Festlegungen von Verantwortlichkeiten im Datenschutz, z. B.:

- Festlegung der Abteilung, des Sachgebietes etc. welches für die Verarbeitung der Daten zuständig ist,
- Evtl. Festlegungen zur Auftragsdatenverarbeitung (vgl. § 7 SächsDSG),
- Frühzeitige Einbeziehung des behördlichen Datenschutzbeauftragten (falls bestellt) in die Verfahrenseinführung bzw. bereits zum Zeitpunkt der Verfahrensausschreibung.

Weitere Informationen:

- BSI-Grundschutz, Baustein M2.502 Regelung der Verantwortlichkeiten im Bereich Datenschutz
- Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Bestellung von Datenschutzbeauftragten öffentlicher Stellen

2. Sicherstellung der Verpflichtung gemäß § 6 SächsDSG

Verpflichtung der Mitarbeiter auf das Datengeheimnis

Weitere Informationen:

- Merkblatt des Sächsischen Datenschutzbeauftragten zur Verpflichtung auf das Datengeheimnis

3. Verfahrensverzeichnis gemäß § 10 SächsDSG erstellen

Weitere Informationen:

- Bekanntmachung des Sächsischen Datenschutzbeauftragten zum Verzeichnis automatisierter Verarbeitungsverfahren

4. Vorabkontrolle gemäß § 10 Abs. 4 SächsDSG durchführen

Weitere Informationen:

- Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Vorabkontrolle

5. Festlegungen in Datenschutz- und Informationssicherheitskonzepten

Ziel des Einsatzes und rechtlichen Rahmen des eingesetzten Verfahrens dokumentieren

- Nennung des Zwecks zum Einsatz des Verfahrens
- Aufführen der rechtlichen Grundlage zur Verarbeitung der personenbezogenen Daten
- Bei Verarbeitung auf der Grundlage der Einwilligung des Betroffenen: Klärung, dass die Verarbeitung der Daten zur Erfüllung gesetzlich vorgeschriebener Aufgaben erforderlich ist.

Festlegung der zu verarbeitenden personenbezogenen Daten (Bürger- und Mitarbeiterdaten)

- Der Umfang der personenbezogenen Daten, die bei einer E-Government-Anwendung verarbeitet werden sollen, ist im Datenschutzkonzept festzulegen. Die zu verarbeitenden personenbezogenen Daten sind abschließend aufzuzählen.
- Erforderlichkeit für die Aufgabenerfüllung prüfen
- Prüfung der Geeignetheit der Daten
- Grundsatz der Zweckbindung gewährleisten
- Grundsätze der Datenvermeidung und Datensparsamkeit gewährleisten
  - Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass die Verarbeitung personenbezogener Daten nur im erforderlichen Rahmen stattfindet, indem z. B. nur die erforderlichen Daten verarbeitet werden oder sogar auf einen Personenbezug verzichtet wird.
  - Soweit rechtlich und technisch möglich und zumutbar, ist den Betroffenen zu ermöglichen, anonym oder pseudonym zu handeln oder pseudonym zu bezahlen. Hierfür können unterschiedliche Zahlungsverfahren genutzt werden, die diese Möglichkeit bieten.
- Ist eine Anonymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System / Teilsystem oder den jeweiligen Arbeitsschritt eine entsprechende Prozedur zu finden, die die personenbezogenen Daten frühestmöglich anonymisiert bzw. pseudonymisiert (siehe hierzu auch Orientierungshilfe »Datenschutzfreundliche Technologien« des Arbeitskreises »Technik« der Datenschutzbeauftragten des Bundes und der Länder).

Ermittlung des Schutzbedarfes der verarbeiteten Daten pro Schutzziel gemäß § 9 Abs. 2 SächsDSG

Weitere Informationen:

- Hinweise zur Schutzbedarfsfeststellung im BSI-Standard 100-2

Aufzählung und Beschreibung der eingesetzten IT-Komponenten

- Aufzählung und zumeist grafische Darstellung der eingesetzten technischen Komponenten
- Darstellung und Dokumentation, in welcher Weise die Komponenten miteinander in Verbindung stehen
- Darstellung der Einbettung der technischen Komponenten in die Gesamt-IT-Infrastruktur

Prozessbezogene Verfahrensbeschreibung, in der die Verfahrensweisen bei der Verarbeitung der personenbezogener Daten vollständig und aktuell dokumentiert sind

- Konkrete Beschreibung, wie die personenbezogenen Daten verarbeitet werden

Dokumentation der Festlegung der erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzrechtlichen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionssicherheit, Transparenz)

- Konkrete Maßnahmen aufführen und beschreiben, die die Vertraulichkeit sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Vertraulichkeit z. B. festzulegen:

  - Sicherstellung, dass eine Kenntnisnahme von personenbezogenen Daten nur durch gesetzlich dazu Befugte erfolgt
  - Differenzierte Zugriffsrollen und -rechte mit Vertretungsregelungen
  - Zutritts- und Zugriffsregelungen durch Passwörter, Chipkarten u. ä.
  - Bildschirmschoner mit Passwort
  - Regelungen für sicheres Löschen

- Konkrete Maßnahmen aufführen und beschreiben, die die Integrität sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Integrität z. B. festzulegen:

  - Daten dürfen nicht unbefugt geändert werden
  - Differenzierte Schreibrechte bei elektronischen Daten
  - Beschränkte Vergabe von Administratorbefugnissen
  - Verschlüsselung bei besonderen Risiken:
  - Mobile Technik / Datenträger
  - Heimarbeit
  - WLAN
  - Internet / E-Mail

- Konkrete Maßnahmen aufführen und beschreiben, die die Verfügbarkeit sicherstellen. Zur Feststellung der Anforderungen an die Verfügbarkeit sind z. B. folgende Fragen zu klären:

  - Wie lange kann höchstens auf den Rechner bzw. die Daten verzichtet werden (Stunden, Tage oder Wochen)?
  - Welcher Termin ist der kritischste für den Ausfall des Rechners oder den Verlust der Daten?
  - Welche Folgen hat ein längerfristiger Rechnerausfall?
  - Welcher Schaden tritt ein, wenn Daten endgültig verloren sind?
  - Wie lange dauert es und wie viel kostet es, das System wiederherzustellen oder die Daten erneut zu erfassen?

- Konkrete Maßnahmen aufführen und beschreiben, die die Authentizität sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Authentizität z. B. festzulegen:

  - Vergabe von Benutzernamen und Passwort, Verwendung von Chipkarten
  - Verwendung von qualifizierten elektronischen Signaturen gemäß § 1 SächsVwVfZG i. V. m. § 3a Absatz 2 VwVfG

- Konkrete Maßnahmen aufführen und beschreiben, die die Revisionsfähigkeit sicherstellen. Je nach Schutzbedarf sind zur Sicherstellung der Revisionsfähigkeit z. B. festzulegen:

  - Umfang des Protokolls
  - Anlass, Zweck und Zeitpunkt der Protokollauswertung
  - Ablauf der Protokollauswertung
  - Befugte, die die Protokolle auswerten
  - Löschung der Protokolle
  - In der Regel Dienstvereinbarung

- Konkrete Maßnahmen aufführen und beschreiben, die die Transparenz sicherstellen:

- Das Transparenzgebot wird z. B. durch Unterrichtungspflichten über die Möglichkeit anonymen und pseudonymen Handelns, über Profilbildungen gewährleistet. Diese Informationen sollten in einer Datenschutzerklärung zusammengefasst und den Nutzern zugänglich gemacht werden.

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

- Es ist festzulegen, wie die o. g. Rechte der Betroffenen vom Verfahren gewährleistet werden, z. B. wie beauskunftet wird.
- Auf die systemseitige Gewährleistung der Betroffenenrechte sollte schon bei der Ausschreibung des Verfahrens geachtet werden.
- Die Datenschutzhinweise sollten eine Erklärung enthalten zu Grundsätzen der Verfahrensweise bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Angebots im Internet anfallen. Außerdem sollte über die Auskunftsansprüche und Korrekturrechte informiert werden. Die Hinweise sollten an zentraler Stelle – etwa auf der Eingangsseite im Internet – erscheinen und leicht verständlich formuliert sein. Zur Gewährleistung der Transparenz gehört insbesondere die Information darüber, wer für die Gestaltung des Angebots verantwortlich zeichnet.
- Wenn die Nutzung eines Angebots die Erhebung personenbezogener Daten voraussetzt, sind die Nutzer über die Zweckbestimmung der Verarbeitung, für die die Daten bestimmt sind, zu unterrichten.
- Bei elektronischer Antragsstellung ist der Antragsteller darüber zu informieren, wie das Gesamtverfahren abgewickelt wird.

Weitere Informationen:

- BSI-Grundschutz, Baustein B 1.5 Datenschutz

Rollen und Zugriffsrechte festlegen

- Wenn verschiedene Stellen bei der Erbringung einer E-Government-Dienstleistung zusammenwirken, ist darauf zu achten, dass die beteiligten Einrichtungen nur die für die jeweilige Teilaufgabe erforderlichen Daten zur Kenntnis nehmen können.
- Es muss sichergestellt sein, dass nur berechtigte Nutzer den Zugang zu den Daten haben. Die Identifizierung und Authentisierung sollte an zentraler Stelle durchgeführt werden (Authentifizierungsserver) bzw. über das jeweilige Betriebssystem erfolgen.
- Rechte sind sowohl benutzerbezogen als auch datei- oder programmbezogen zu vergeben, um die Zugriffsmöglichkeiten zweckgebunden zu begrenzen. Dabei ist der Maßstab immer das fachliche Anforderungsprofil und die Arbeitsaufgabe des einzelnen Benutzers.
- Arbeitsschritte, die im Hinblick auf die Einhaltung der Zweckbindung besonders sensibel sind, sind zu Zwecken der Beweissicherung soweit notwendig zu protokollieren. Beweissicherung bedeutet in diesem Zusammenhang, dass es im Nachhinein möglich sein muss, den Missbrauch zugestandener Rechte nachzuweisen oder die versuchte Ausübung von nicht zugestandenen Rechten aufzudecken.

- Daten sind logisch getrennt zu speichern. In diesem Fall ist eine gegenseitige Abschottung der zweckgebundenen Datenbestände am einfachsten und am datenschutzfreundlichsten zu realisieren.
- Moderne Datenverarbeitungsanlagen bieten die Möglichkeit, gleichzeitig mehrere Anwendungen abzuarbeiten. Hier ist darauf zu achten, dass die einzelnen Anwendungen und ihre jeweils zweckgebundenen Daten gegenseitig voneinander abgeschottet verarbeitet werden. Dies kann in der Praxis durch den Einsatz technischer Zusatzsysteme erreicht werden, die beispielsweise auf einem Prozessor mehrere virtuelle Maschinen simulieren, welche die jeweiligen Anwendungen einschließlich deren Daten gegeneinander abgekapselt verarbeiten.
- Sensible Daten sind verschlüsselt zu speichern und zu übertragen, damit eine inhaltliche Kenntnisnahme der Daten durch Unbefugte verwehrt wird. Die Prozeduren der Verschlüsselung sind für die Benutzer transparent zu halten.
- Für besondere Zwecke erhobene Daten sollten mit einem spezifischen Kennzeichen versehen werden, welches den Zweck ihrer Erhebung sowie einer eventuellen Verarbeitung und Übermittlung spezifiziert, sodass eine Verwendung für einen anderen Zweck kontrolliert werden kann. Die Vergabe solcher Kennzeichen und die Sicherung der Zweckbindung anhand der Auswertung dieser Kennzeichen, stellt eine elegante und zukunftsorientierte Sicherheitstechnologie dar. Für ihre technische Realisierung wären allerdings erhebliche Änderungen bzw. Erweiterungen der bestehenden Betriebs- und Datenbanksysteme sowie Anwendungsprogramme erforderlich, die derzeit noch nicht über solche Funktionalitäten verfügen.

Festlegungen zur Löschung von Daten

Es ist festzulegen,

- Welche Löschregeln für welche Datenbestände gelten,
- Wie aus den Löschregeln die Umsetzung der Löschung in Prozessen der verantwortlichen Stelle erreicht wird,
- Wie die Löschregeln, Umsetzungsvorgaben und durchgeführten Löschmaßnahmen zu dokumentieren sind,
- Wer für die aus dem Löschkonzept entstehenden Aufgaben der Umsetzung, Überprüfung und Fortschreibung verantwortlich ist.

Weitere Informationen:

- Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“

Festlegungen zur Protokollierung

- Erhebung, Verarbeitung und Weitergabe von personenbezogenen Daten (Bestands-, Verbindungs- und Nutzungsdaten) sollten grundsätzlich anonymisiert oder mittels eines Pseudonyms erfolgen.
- Für Art, Umfang und Aufbewahrung der Protokollierung und Bestandsdaten gilt der Grundsatz der Erforderlichkeit. Die Protokollierung sollte so erfolgen, dass sensitive Aktivitäten und vorab

zu definierende Systemzustände für eine nachfolgende Kontrolle festgehalten werden. Unter anderem sollte Folgendes protokolliert werden:

- Systemgenerierung und Modifikation von Systemparametern,
- Einrichten von Benutzern,
- Erstellung von Rechteprofilen,
- Einspielen und Änderung von Anwendungssoftware,
- Änderungen an der Dateiorganisation,
- Durchführung von Datensicherungsmaßnahmen,
- Sonstiger Aufruf von Administrations-Tools,
- Datenübermittlungen,
- Zugriffe auf aktive Systemkomponenten,
- Falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen, insbesondere sicherheitskritische Zugriffe mit oder ohne Erfolg,
- Verteilung der Rechner- / Systemlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance,
- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können.

- Protokolldaten dürfen nur zu Zwecken genutzt werden, die Anlass für ihre Speicherung waren.
- Die Daten über die Inanspruchnahme verschiedener Online-Dienste werden getrennt gespeichert.
- Eine unzulässige Zusammenführung der Nutzungsdaten ist technisch zu verhindern.
- Die Protokolldaten werden bei kostenfreier Nutzung des Online-Dienstes nach Ende der jeweiligen Nutzung gelöscht. Bei kostenpflichtiger Nutzbarkeit sind die Protokolldaten spätestens nach Ablauf von sechs Monaten nach Versendung der Rechnung und des Einzelnachweises zu löschen, soweit es nicht zu Einwendungen gekommen ist oder nach bereichsspezifischen Regelungen besondere Aufbewahrungsfristen zu beachten sind.
- Die Verwendung von Protokolldaten zu Zwecken der Verhaltens- und Leistungskontrolle ist untersagt. Nur im Einzelfall ist eine Auswertung der Protokolldaten zur Aufdeckung von Missbräuchen zulässig.

Weitere Informationen:

- Orientierungshilfe „Protokollierung“ vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Festlegungen zur Auftragsdatenverarbeitung

- Den Regeln der Auftragsdatenverarbeitung entsprechend, muss für jedes »Outsourcing-Vorhaben« ein schriftlicher Auftrag erteilt werden. Darin sind insbesondere darzustellen:
  - Detaillierte Festlegung der Rechte und Pflichten der Daten verarbeitenden Stelle und des Auftragnehmers
  - Gegenstand und Umfang der übertragenen Tätigkeiten
  - Die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Datenschutzmaßnahmen

  - Etwaige Unterauftragsverhältnisse des Auftragnehmers
- Ferner muss vereinbart werden, dass der Auftraggeber dem Auftragnehmer Weisungen hinsichtlich der Verarbeitung personenbezogener Daten erteilen darf.
- Das Personal des beauftragen Unternehmens ist auf das Datengeheimnis nach § 6 SächsDSG zu verpflichten.
- In der Vereinbarung ist ferner festzulegen, dass der Auftragnehmer sich der Kontrolle der zuständigen staatlichen Datenschutzaufsichtsbehörde und des Auftraggebers unterwirft; dabei sind die Vorgaben des jeweils einschlägigen Datenschutzgesetzes zu beachten.
- Vor allem bei größeren Projekten bietet es sich an, die technisch-organisatorischen Maßnahmen in einem Datenschutz- und Sicherheitskonzept zusammenzufassen, dessen Umsetzung und Einhaltung vertraglich vereinbart wird. Die technisch-organisatorischen Maßnahmen können dann dem Stand der Technik folgend fortgeschrieben werden, ohne dafür den »Outsourcing-Vertrag« selbst ändern zu müssen.

Weitere Informationen:

- Mustervertrag zur Auftragsdatenverarbeitung gemäß § 7 SächsDSG

F. Anlage 3: Dienstleister zur Erstellung und Zertifizierung barrierefreier Webseiten

Die aufgeführten Adressen erheben keinen Anspruch auf Vollständigkeit.

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

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-Gebaerden-sprache.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

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

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

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