UNIKASSEL
VERSITÄT

Ass. iur. Maxi Nebel

Universität Kassel
Pfannkuchstr. 1
34109 Kassel

Telefon +49 561 804 6091
Fax +49 561 804 6081

Stellungnahme

zur öffentlichen Anhörung im Innenausschuss des Sächsischen Landtags

zum Bericht über die Evaluierung des Sächsischen E-Government-Gesetzes (SLT-Drs. 6/9859)

30. November 2017

ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

provet Projektgruppe verfassungsverträgliche Technikgestaltung

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

Vorbemerkung

Das Sächsische E-Government-Gesetz (SächsEGovG)[1] ist seit 2014 in Kraft und damit nach Erlass des E-Government-Gesetzes des Bundes (EGovG-Bund)[2] aus dem Jahre 2013 das erste Landesgesetz, welches diese Vorschriften auf Landesebene adressiert. Nach Schleswig-Holstein ist es bundesweit das zweite Landesgesetz zur Schaffung einer elektronischen Verwaltung überhaupt. Der möglichst frühe Erlass eines E-Government-Gesetzes durch den sächsischen Gesetzgeber ist sehr zu begrüßen. Neben der Adressierung der Vorschriften aus dem E-Government-Gesetz des Bundes sind auch eigenständige Akzente gesetzt, die über dieses hinausgehen. Gerade solche hatten eine wichtige Vorbildfunktion auch für andere Bundesländer, etwa Nordrhein-Westfalen.

Das Sächsische E-Government-Gesetz ist durchaus geeignet, eine medienbruchfreie elektronische Verwaltung zu etablieren, die sich an den Lebensverhältnissen der Bürgerinnen und Bürger sowie den Bedürfnissen von Unternehmen orientiert. Die in § 21 SächsEGovG vorgesehene frühzeitige Evaluierung nach einer dreijährigen Übergangszeit ist hilfreich, um die Zielsetzungen zu prüfen sowie frühzeitig Gegenmaßnahmen zu ergreifen, wo eine Fehlentwicklung absehbar ist. Einige Punkte werden im Folgenden eruiert.[3]

Zu 1:
Elektronische Kommunikation, § 2 Abs. 1 Satz 1 und 3 SächsEGovG

§ 2 Abs. 1 SächsEGovG verpflichtet staatliche Behörden und Träger der Selbstverwaltung zur Ermöglichung der elektronischen Kommunikation (Satz 1) unter grundsätzlicher Anwendung von Verschlüsselungsverfahren (Satz 3). Die Vorschrift geht damit über das Bundesgesetz hinaus, das keine Kommunikationsverschlüsselung vorsieht. Die Regelung ist sachgerecht, da Behörden bereits aus Gründen des Grundrechtsschutzes verpflichtet sind,[4] Verschlüsselungsverfahren für die elektronische Kommunikation – möglichst mit offenen Standards – anzubieten und zu nutzen. Dazu gehört zum Beispiel öffentliche Schlüssel bekannt zu geben und Entschlüsselungsprogramme vorzuhalten, um eingehende Nachrichten entschlüsseln zu können.

Laut Evaluierungsbericht ist die elektronische Kommunikation mit den Behörden im Sinne des Satz 1 mittels E-Mail oder Online-Kontaktformular flächendeckend ermöglicht. Der Bericht legt jedoch nahe, dass noch keine ausreichende Verschlüsselungsquote im Sinne des Satz 3 erreicht wurde. Neben De-Mail als Möglichkeit verschlüsselter Kommunikation wäre es förderlich, sowohl s/mime als auch PGP anzubieten. Beide Verfahren sind in der Bevölkerung weit verbreitete Public-Key-gestützte E-Mail-Verschlüsselungsverfahren. Das bietet den Vorteil, das Bürgerinnen und Bürger auf eigene Veranlassung hin mit der Behörde verschlüsselt kommunizieren können, ohne einen De-Mail-Zugang vorhalten zu müssen. Zudem sind vielfältige, auf s/mime oder OpenPGP basierende Verschlüsselungsverfahren mit diesen Standards kompatibel, zum Beispiel die Volksverschlüsselung.[5]

Zugleich sollte „grundsätzlich“ aus § 2 Abs. 1 Satz 3 SächsEGovG gestrichen werden, so dass Verschlüsselungsverfahren in der elektronischen Kommunikation zwingend anzuwenden sind. Das sorgt für Klarheit in der praktischen Anwendung und vermeidet langwierige und damit ressourcen-

---

1 Sächsisches E-Government-Gesetz vom 9. Juli 2014, SächsGVBl. 2014, Nr. 11, S. 398.

2 E-Government-Gesetz vom 25. Juli 2013, BGBl. I S. 2749.

3 Die Nummerierung im Folgenden bezieht sich im Wesentlichen auf Kapitel C I des Evaluierungsberichts der Staatsregierung, SLT-Drs. 6/9859, S. 15 ff.

4 S. zu staatlichen Schutzpflichten z. B. *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, Kassel 2016, S. 14 ff. mit weiteren Nachweisen.

5 Eine Verschlüsselungssoftware des Fraunhofer SIT in Darmstadt in Kooperation mit der Deutschen Telekom, https://volksverschluesselung.de/.

intensive Diskussionen zu der Frage, was unter „grundsätzlich“ zu verstehen ist und ob und warum ein Kommunikationsvorgang im Einzelfall keiner Verschlüsselung bedürfe.

Zudem ist der Einsatz der schriftformersetzenden Verfahren ausbaufähig. Zum einen sollte die Integration der eID-Funktion des neuen Personalausweises ausgeweitet werden. So ist dringend darauf hinzuwirken, für mehr Anwendungen die Möglichkeit der Authentifizierung durch eID zu ermöglichen. Diese war in der Vergangenheit auch bundesweit nur gering. Nur durch ein breites Angebot an Nutzungsmöglichkeiten kann jedoch ein Anreiz für die Bürgerinnen und Bürger geschaffen werden, die eID-Funktion zu akzeptieren und zu nutzen.[6] Gleiches gilt für die Ausweitung des De-Mail-Einsatzes. Der Einsatz der qualifizierten elektronischen Signaturen (QES) sollte forciert werden, die derzeitige Verbreitung in den Kommunen (50 % der befragten Kommunen nutzen QES) und unter den Trägern der Selbstverwaltung (18 % nutzen QES) sind für eine flächendeckende Nutzung elektronischer Kommunikation im Falle eines Schriftformerfordernisses nicht ausreichend.

Es sollte erwogen werden, Behörden und Träger der Selbstverwaltung in § 2 Abs. 1 SächsEGovG explizit zu verpflichten, einen Zugang für die Übermittlung elektronischer Dokumente mit und ohne QES sowie einen De-Mail-Zugang zu eröffnen. Dies ist vergleichbar mit den Regelungen des § 2 EGovG-Bund und § 3 NRWEGovG. § 2 Abs. 2 Nr. 1 SächsEGovG in Verbindung mit § 3a Abs. 2 VwVfG formuliert keine Pflicht zur Eröffnung eines De-Mail-Zugangs, sondern setzt diesen voraus.[7] Das erklärt auch die bisherige geringe Verbreitung und zurückhaltende Nutzung von De-Mail und QES. Eine gesetzliche Pflicht für alle Behörden und Träger der Selbstverwaltung würde einer schnelleren Verbreitung Vorschub leisten. Zu beachten ist in diesem Zusammenhang, dass seit Inkrafttreten der eIDAS-VO[8] im Jahre 2016 für die elektronischen Signaturen die Vorschriften der Art. 25 ff. eIDAS-VO sowie das Vertrauensdienstegesetz (VDG)[9] maßgeblich sind.

Seit dem Inkrafttreten der eIDAS-VO steht juristischen Personen zudem die Verwendung von elektronischen Siegeln nach Art. 35 eIDAS-VO offen. Diese sind mit elektronischen Signaturen vergleichbar und ermöglichen den Herkunftsnachweis einer Erklärung bei einer Institution, wenn keine persönliche Unterschrift einer natürlichen Person notwendig ist. Einem elektronischen Siegel kommt nicht die gleiche Beweiswirkung zu wie qualifizierten elektronischen Signaturen.[10] Für den Einsatz bei der medienbruchfreien elektronischen Kommunikation zwischen Verwaltung und natürlichen oder juristischen Personen und zur Übermittlung von Urkunden, Zeugnissen und Bescheiden sind elektronische Siegel jedenfalls gut geeignet und zudem kostengünstiger als QES.

Im Übrigen ist der Vorbehalt der Bereitstellung von Haushaltsmitteln in § 2 Abs. 2 Satz 1 SächsEGovG zu streichen. Der Einsatz der Systeme für eine medienbruchfreie, umfassende elektronische Verwaltung muss durch eine dauerhafte und bedingungslose Finanzierung sichergestellt sein. Nur so können die unions- und bundesrechtlichen Vorgaben in ausreichendem Maße umgesetzt werden und die elektronische Verwaltung langfristig verwirklicht werden.

---

6 Zum Beispiel zur Authentifizierung bei elektronischen Formularen, vgl. *Johannes*, Elektronische Formulare im Verwaltungsverfahren, MMR 2013, 694.

7 BT-Drs. 17/11473, 33.

8 Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO), ABl. Nr. L 257, 73, ber. ABl. 2015 Nr. L 23, 19 und ABl. 2016 Nr. L 155, 44.

9 Vertrauensdienstegesetz vom 18.Juli 2017, BGBl. I S. 2745.

10 *Roßnagel*, Beweiswirkung elektronischer Vertrauensdienste, MMR 2016, 647 (649).

Zu 2:
Elektronische Zahlungsverfahren, § 3 SächsEGovG
Elektronische Rechnungen

Nach § 3 SächsEGovG müssen staatliche Behörden und die Träger der Selbstverwaltung elektronische Zahlungen ermöglichen. Ziel ist es, elektronische Zahlungsverfahren in den Verwaltungsablauf zu integrieren, um eine medienbruchfreie Abwicklung von Verwaltungsverfahren zu ermöglichen. Ausweislich des Evaluierungsberichts ist diese Rechtspflicht durch die Möglichkeit von Überweisung, SEPA-Lastschrift, Kredit- und EC-Kartenzahlung bereits erfüllt, kann aber durch die Integration weiterer Bezahlverfahren in der entsprechenden Basiskomponente[11] erweitert werden.

Die Vorschrift sollte – zur Wahrung der Grundrechte der Bürgerinnen und Bürger – zusätzlich hervorheben, dass es sich bei dem Zahlungsmittel um ein gängiges und hinreichend sicheres Zahlungsmittel handeln muss, insbesondere um die Anforderungen an den Datenschutz und die Datensicherheit zu gewährleisten. Entsprechende Vorgaben finden sich etwa auch in § 4 EGovG-Bund und § 7 NRWEGovG.

Das Sächsische E-Government-Gesetz trifft darüber hinaus keine Aussage zu elektronischen Rechnungen. Rechnungen für öffentliche Aufträge müssen nach der eRechnungs-Richtlinie[12] elektronisch empfangen und verarbeitet werden können; die Richtlinie ist für zentrale Regierungsbehörden als öffentliche Auftraggeber bis 27. November 2018 umzusetzen. Eine Rechnung ist elektronisch, wenn sie in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird, das ihre automatische und elektronische Verarbeitung ermöglicht.[13] Elektronische Rechnungen sind seit dem 1. Juli 2011 in Deutschland durch Änderung des § 14 Umsatzsteuergesetzes (UStG)[14] klassischen Papierrechnungen gleichgestellt, um Geschäftsprozesse einfacher und effizienter zu machen. Das Sächsische E-Government-Gesetz sollte um einen neuen § 3a ergänzt werden, in dem alle Behörden verpflichtet werden, elektronische Rechnungen empfangen und verarbeiten zu können. Die Pflicht gilt nur zur Entgegennahme von elektronischen Rechnungen bei der Vergabe von öffentlichen Aufträgen. Anzuraten ist zudem, Behörden zur Ausstellung von elektronischen Rechnungen, Kosten- und Gebührenbescheiden bei der Durchführung der elektronischen Zahlungsverfahren nach § 3 SächsEGovG zu verpflichten, wenn der Verwaltungskunde dies wünscht. Dadurch würde auch im Verwaltungsverfahren mit Bürgerinnen und Bürgern ein medienbruchfreier Ablauf unterstützt.

Zu 3:
Elektronische Vorgangsbearbeitung und Aktenführung, § 12 SächsEGovG

Einführung der elektronischen Vorgangsbearbeitung, § 12 Abs. 1 SächsEGovG

§ 12 Abs. 1 Satz 1 SächsEGovG verpflichtet staatliche Behörden, elektronische Vorgangsbearbeitung und Aktenführung einzusetzen. Die hierfür eingesetzte Basiskomponente sollte ein umfassendes elektronisches Verwaltungsverfahren ermöglichen. Dies geht über eine bloße elektronische Aktenführung hinaus und beinhaltet alle zur Abwicklung eines Verwaltungsverfahrens notwendigen

---

11 Basiskomponenten sind vom Freistaat Sachsen zentral bereitgestellte E-Government-Anwendungen, die der fachunabhängigen oder fachübergreifenden Unterstützung der Verwaltungstätigkeit dienen; mehr dazu unter Punkt 5.

12 Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen, ABl. EU vom 6. Mai 2014, L 133, 1.

13 Art. 2 Nr. 1 RL 2014/55/EU; vgl. § 4a Abs. 2 EGovG-Bund und Art. 5 Abs. 2 Satz 2 BayEGovG.

14 Zur Umsetzung der Richtlinie 2010/45/EU über das gemeinsame Mehrwertsteuersystem hinsichtlich der Rechnungsstellungsvorschriften, ABl. EU vom 22. Juli 2010, L189, 1.

Schritte zwischen Behörde und Bürger oder Unternehmen, zum Beispiel eine Einbindung elektronischer Formulare ähnlich § 13 EGovG-Bund, die Möglichkeit der Einreichung elektronischer Nachweise oder die Möglichkeit zum Empfang elektronischer Rechnungen. Zudem sollten elektronische Vertrauensdienste im Sinne der eIDAS-VO eingebunden werden, also qualifizierte elektronische Signaturen, Siegel, Zeitstempel und Einschreibebestätigungen. Darüber hinaus sollte auch die Ausübung von Verfahrensrechten durch die Verwaltungskunden integriert werden, denn die Einräumung digitaler Rechte stärkt einerseits die Stellung der Bürgerinnen und Bürger und steigert andererseits deren Akzeptanz des E-Government.

Eine Regelung wie § 13 EGovG-Bund bezüglich elektronischer Formulare fehlt bisher im Sächsischen E-Government-Gesetz. Eine solche schafft Klarheit für Bürgerinnen und Bürger sowie die Verwaltung und erleichtert die Abschaffung gelebter Schriftformerfordernisse, wo diese nicht zwingend gesetzlich vorgeschrieben sind. Für ein medienbruchfreies Verwaltungshandeln ist dies äußerst förderlich und wirkt sich auch positiv auf die Möglichkeiten des ersetzenden Scannens aus (dazu siehe unten).

§ 12 Abs. 1 Satz 2 SächsEGovG verpflichtet zur Einhaltung der Grundsätze ordnungsgemäßer Aktenführung und ordnungsmäßiger Aufbewahrung. In dieser Vorschrift sollte ein Hinweis aufgenommen werden, dass dabei der Stand der Technik einzuhalten ist. Ein solcher Verweis führt regelmäßig zu den Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI), etwa zu BSI TR-03125 (TR-ESOR), die den Stand der Technik hinsichtlich des Erhalts des Beweiswertes elektronisch signierter Dokumente bildet. Zudem wäre es aus Datensicherheitsaspekten sinnvoll, Behörden zur Gewährleistung der Datensicherheitsziele (Integrität, Authentizität, Vertraulichkeit, Vollständigkeit etc.) explizit zu verpflichten, um insbesondere besonders schützenswerte Daten dauerhaft ausreichend zu sichern. Hinsichtlich der langfristigen Erhaltung von QES ist zudem § 15 VDG zu beachten, der vorschreibt, dass qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten bei Bedarf durch geeignete Maßnahmen nach dem Stand der Technik neu zu schützen sind, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird.

Übermittlung elektronischer Daten und Akten, § 12 Abs. 2 SächsEGovG

§ 12 Abs. 2 SächsEGovG regelt die elektronische Vorgangsbearbeitung und Aktenführung zwischen Behörden. Mit Wirksamwerden der Datenschutz-Grundverordnung[15] und dem neuen Bundesdatenschutzgesetz (BDSG n. F.)[16] zum 25. Mai 2018 sind die entsprechenden Vorgaben zu beachten. Das gilt insbesondere für § 25 Abs. 1 BDSG n. F. zu den datenschutzrechtlichen Grundlagen der Übermittlung von personenbezogenen Daten zwischen öffentlichen Stellen. Ein entsprechender Hinweis in § 12 Abs. 2 SächsEGovG ist sinnvoll.

Die gesetzlichen Pflichten des § 12 Abs. 1 und 2 SächsEGovG sollten nicht unter den Vorbehalt der Bereitstellung von Haushaltsmitteln gestellt werden. Die elektronische Vorgangsbearbeitung und Aktenführung muss durch dauerhafte und bedingungslose Finanzierung sichergestellt sein, um unions- und bundesrechtliche Vorgaben in ausreichendem Maße umzusetzen und die elektronische Verwaltung langfristig zu verwirklichen.

---

15 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU vom 4. Mai 2016, L 119, 1.

16 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU), BGBl. I vom 5. Juli 2017, 2097.

Elektronische Akteneinsicht, § 12 Abs. 3 SächsEGovG

Das Recht zur medienbruchfreien und medienunabhängigen Akteneinsicht nach § 12 Abs. 3 SächsEGovG entspricht § 8 EGovG-Bund. Bei der Datenübermittlung an nichtöffentliche Stellen sind die datenschutzrechtlichen Vorgaben zu beachten. Ab 25. Mai 2018 ist hier insbesondere § 25 Abs. 2 BDSG n. F. anzuwenden. Zu beachten ist, dass die derzeitige Fassung des § 25 Abs. 2 Satz 1 Nr. 2 BDSG n. F. mangels Öffnungsklausel in der Datenschutz-Grundverordnung nicht mit dieser konform und daher nicht anwendbar ist.[17] Weiterhin ist bei der Datenübermittlung sicherzustellen, dass Daten nicht unbefugt eingesehen und vervielfältigt werden können und die Datensicherheitsziele (Integrität, Authentizität, Vertraulichkeit, Vollständigkeit etc.) gewährleistet sind.

Ersetzendes Scannen, § 12 Abs. 4 SächsEGovG

§ 12 Abs. 4 Satz 1 SächsEGovG ermöglicht das ersetzende Scannen eingereichter Schriftstücke. Satz 2 regelt Modalitäten der Umsetzung des ersetzenden Scannens. Satz 3 erlaubt die Vernichtung des Originals, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist. Diese Vorschrift ist in der Praxis noch nicht ausreichend umgesetzt, so dass nach wie vor unnötig Originalschriftstücke aufbewahrt und teils Doppelakten geführt werden. Dies entspricht nicht dem Grundsatz der Sparsamkeit und Wirtschaftlichkeit und erhöht das Fehlerpotenzial im Verwaltungshandeln. Zweifel bestehen in der Praxis vor allem hinsichtlich der Modalitäten des ersetzenden Scannens.

Notwendig ist zunächst, in Satz 2 aufzunehmen, dass der gesamte Prozess des ersetzenden Scannens dem Stand der Technik zu entsprechen hat (vgl. § 7 EGovG-Bund, § 10 Abs. 1 Satz 2 NRWEGovG, § 7 Abs. 3 Satz 3 BayEGovG). Die BSI TR-03138 (TR-RESISCAN) des BSI entspricht dem Stand der Technik für ersetzendes Scannen. Sie enthält technische und organisatorische Maßnahmen und Anforderungen an die Vorbereitung und Durchführung des Scanprozesses und wird ergänzt durch die TR-ESOR zur beweiswerterhaltenden Aufbewahrung elektronischer Dokumente. Durch die TR-RESISCAN werden rechtssichere Scanlösungen ermöglicht. Werden die Anforderungen und Maßnahmen der TR-RESISCAN umgesetzt, ist der Beweiswert gescannter Dokumente hoch und das Risiko eines Beweisverlustes durch die Vernichtung eines Originaldokumentes im Vergleich zu den Vorteilen des ersetzenden Scannens hinnehmbar gering.

Die Beweiswerterhaltung wird auch durch § 371b ZPO gestützt. Scannt eine Behörde oder eine mit öffentlichem Glauben versehene Person öffentliche Urkunden nach dem Stand der Technik und liegt eine Bestätigung (Transfervermerk) der bildlichen und inhaltlichen Übereinstimmung vor, finden die Vorschriften zur Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Sind Dokument und Transfervermerk qualifiziert elektronisch signiert, gilt sogar die Vermutung der Echtheit der Urkunde gemäß § 437 ZPO. Bei einem qualifizierten elektronischen Siegel oder Zeitstempel gilt zudem die Vermutung des Art. 35 Abs. 2 bzw. Art. 41 Abs. 2 eIDAS-VO.

Die Beweiskraft gescannter Dokumente konnte bisher von Gerichten nur selten beurteilt werden. Einzig das VG Wiesbaden hat sich in der Vergangenheit mit – jedoch schwerwiegenden – Verstößen gegen einen ordnungsgemäßen Scanprozess beschäftigt.[18] Dass nach dem Stand der Technik ersetzend gescannte Dokumente von Gerichten anerkannt werden können, wurde im Jahr 2014 in einer Simulationsstudie in vierzehn Fällen erprobt.[19] Die Simulationsstudie hat gezeigt, dass auch

---

17 *Nebel*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Baden-Baden 2018, § 3 Rn. 115.

18 VG Wiesbaden, NJW 2014, 2060 sowie VG Wiesbaden, NVwZ 2015, 238.

19 Zusammenfassend *Roßnagel/Nebel*, Beweisführung mittels ersetzend gescannter Dokumente, NJW 2014, 886; ausführlich *dies.,* Simulationsstudie Ersetzendes Scannen, 2014, www.uni-kassel.de/uni/fileadmin/datas/uni/presse/anhaenge/2014/SIM.pdf.

mit gescannten Dokumenten Beweis geführt werden kann. Sie hat gezeigt, dass der Beweiswert erhöht wird, wenn die Empfehlungen der TR-RESISCAN eingehalten und dies durch Zertifizierung oder Transfervermerk nachgewiesen werden kann. Die vierzehn Beweisaufnahmen und Beweisentscheidungen der Simulationsstudie sind weder repräsentativ noch binden sie andere Gerichte. Dennoch können die entsprechenden Erfahrungen wegweisend wirken und bieten einen großen Zugewinn an Einschätzungssicherheit.

Überführung in andere Dateiformate, § 12 Abs. 5 SächsEGovG

§ 12 Abs. 5 SächsEGovG ermöglicht und fordert die Übertragung in ein anderes elektronisches Format, soweit dies zur Erhaltung der Lesbarkeit erforderlich ist. Hier sollte verdeutlicht werden, dass alle elektronischen Dokumente möglichst bald in ein langfristig lesbares Format wie zum Beispiel PDF/A übertragen werden, um dem Grundsatz ordnungsgemäßer Aufbewahrung und Langzeitarchivierung zu entsprechen.

Zu 4: Information/Transparenz

Zu 4.1: Amtliche Mitteilungs- und Verkündungsblätter, § 4 SächsEGovG

§ 4 Abs. 3 SächsEGovG regelt die Notwendigkeit der Unkenntlichmachung personenbezogener Daten nach Zweckerledigung in den elektronischen Fassungen der behördlichen Publikationen. Die Regelung ist ohne Vorbild in anderen E-Government-Gesetzen. Bei der Umsetzung der Vorschrift bestehen laut Evaluierungsbericht erhebliche Unsicherheiten sowohl technischer als auch rechtlicher Art. Insbesondere erwägt die Staatsregierung, die Vorschrift zu streichen, da sie die elektronische Publikation erschwert und eine vergleichbare Vorschrift in anderen Bundesländern und im Bund nicht vorhanden ist.

Hierbei ist jedoch anzumerken, dass die jeweiligen Behörden nicht von der Verpflichtung zur Löschung von Daten entbunden sind, auch wenn in anderen Landesgesetzen und im Bundesgesetz entsprechende Vorschriften fehlen. Sofern nicht eine Archivierungspflicht besteht, ergeben sich Löschpflichten aus den allgemeinen datenschutzrechtlichen Vorschriften, derzeit § 20 Sächsisches Datenschutzgesetz (SächsDSG). Nach Wirksamwerden der Datenschutz-Grundverordnung gilt Art. 17 Abs. 1 DSGVO.[20] Darüber hinaus ergibt sich eine entsprechende Pflicht zum Löschen aus den allgemeinen Grundsätzen der Datenminimierung und Datensparsamkeit[21] sowie der Speicherbegrenzung. Die besondere Gefährdungslage für elektronische Daten gegenüber Papierdaten erfordert ein strengeres Vorgehen als bei Papierdokumenten. Daher ist weniger über eine gesetzliche Anpassung der Vorschriften nachzudenken als über handhabbare organisatorische und technische Lösungen. Eine Handreichung oder Auslegungshilfe zu den Vorgaben des Art. 17 Abs. 1 DSGVO und § 4 Abs. 3 SächsEGovG ist hier notwendig, um ein einheitliches Vorgehen sicherzustellen.

---

20 S. dazu *Hohmann/Miedzianowski*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Baden-Baden 2018, § 4 Rn. 1 ff.

21 Auch wenn die Datensparsamkeit nicht mehr explizit als allgemeiner Grundsatz der Datenverarbeitung in Art. 5 Abs. 1 DSGVO aufgeführt ist, findet sie weiterhin Anwendung, s. dazu *Husemann*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Baden-Baden 2018, § 5 Rn. 41 ff.

Zu 5:
Zentrale Infrastruktur – Basiskomponenten, § 10 Abs. 2 und 4 SächsEGovG

Die Durchführungsverordnung des Sächsischen E-Government-Gesetzes (SächsEGovGDVO) etabliert eine Nutzungspflicht der bestehenden Basiskomponenten durch staatliche Behörden. Die Basiskomponenten sind gemäß § 10 Abs. 1 Satz 1 SächsEGovG vom Freistaat Sachsen zentral bereitgestellte E-Government-Anwendungen, die der fachunabhängigen oder fachübergreifenden Unterstützung der Verwaltungstätigkeit dienen. Sie stellen eine hervorragende Möglichkeit dar, Verfahren zu standardisieren, langfristig medienbruchfreie Verwaltungsverfahren zu etablieren, die Interoperabilität nach § 9 SächsEGovG zu stärken und dabei die Wirtschaftlichkeit des E-Government zu wahren sowie dessen Leistungsfähigkeit und Effizienz zu steigern. Daher sollte die Ausgestaltung der Basiskomponenten nicht unter den Vorbehalt der Bereitstellung von Haushaltsmitteln gestellt werden. Vielmehr ist ein zügiger Ausbau der Einsatzbreite und ggf. eine weitere Optimierung anzustreben, die sich auf die Wirtschaftlichkeit der elektronischen Verwaltung weiter positiv auswirken.

Der flächendeckende Einsatz solcher Basiskomponenten wirft aber auch datenschutzrechtliche Fragestellungen auf. Insbesondere müssen die Grundsätze der Zweckbindung, Datenminimierung und Datensparsamkeit beachtet werden.[22] Es ist zu evaluieren, welche personenbezogenen Daten für welche Prozesse benötigt werden. Es ist darauf zu achten, dass nur die notwendigen personenbezogenen Daten verarbeitet werden. Zudem ist sicherzustellen, dass betroffene Personen ihre Rechte auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch nach § 5 SächsDSG sowie ab 25. Mai 2018 nach Art. 12 ff. DSGVO mit der Möglichkeit der Beschränkung nach § 7 SächsDSG n. F.[23] wahrnehmen können. Löschkonzepte müssen zudem vorsehen, dass und zu welchem Zeitpunkt personenbezogene Daten bei Zweckerreichung gelöscht werden.

Zu 6:
Interoperabilität, § 9 Abs. 1 und § 13 Abs. 2 SächsEGovG

§ 9 Abs. 1 SächsEGovG verpflichtet staatliche Behörden zur Ausgestaltung ihrer informationstechnischen Systeme in einer Art und Weise, dass ein medienbruchfreier Datenaustausch (Interoperabilität) zwischen ihnen ermöglicht und die Interoperabilität im Verhältnis zu anderen Verwaltungsebenen gefördert wird. Nach § 13 Abs. 2 SächsEGovG sind die gesetzten Standards des IT-Planungsrats für Träger der Selbstverwaltung verbindlich.

Die Interoperabilität ist bisher nur eingeschränkt gewährleistet und sollte weiter ausgebaut werden, um alle Potenziale und Vorteile der elektronischen Verwaltungsarbeit auszunutzen. Behörden sollten weiter sensibilisiert werden, um Standardisierungsoptionen verstärkt zu nutzen. Das setzt jedoch eine noch intensivere landesweite Koordination voraus, insbesondere durch Setzen verbindlicher Vorgaben und Verpflichtungen. Als kontraproduktiv für eine effiziente und langfristig erfolgreiche Umsetzung des Ziels der Interoperabilität scheint der Vorbehalt der Bereitstellung von Haushaltsmitteln, der hier wie oft im Gesetz verankert steht. Dieser ist zu streichen, da Interoperabilität eine wichtige Voraussetzung für eine medienbruchfreie und effiziente elektronische Verwaltung darstellt.

Der medienbruchfreie Datenaustausch zwischen den Behörden wirft aber auch datenschutzrechtliche Fragen auf, die es zu klären gilt. Bei der Datenübermittlung zwischen öffentlichen Stellen sind die Vorgaben des § 14 SächsDSG zu beachten. Ab dem 25. Mai 2018 gelten die Vorgaben der

---

22 *Roßnagel*, in: ders. (Hrsg.), Das neue Datenschutzrecht, Baden-Baden 2018, § 2 Rn. 42 ff.

23 Sächsisches Datenschutzdurchführungsgesetz vom 29. September 2017, SLT-Drs. 6/10918.

Datenschutz-Grundverordnung. Mangels eigener Umsetzungsregelung gilt für die sächsischen Behörden Art. 6 Abs. 1 DSGVO sowie § 6 SächsDSG n. F. zur Verantwortlichkeit der übermittelnden Stelle. Bei Ausführung von Bundesrecht gilt sodann § 25 Abs. 1 BDSG n. F. Dieser erlaubt eine Datenübermittlung durch öffentliche Stellen an andere öffentliche Stellen, wenn dies für die Aufgabenerfüllung des Übermittelnden oder Empfängers erforderlich ist und die Voraussetzungen des § 23 BDSG n. F. vorliegen. Allerdings ist zu beachten, dass § 23 Abs. 1 Nr. 1 und 2 BDSG n. F. unionsrechtswidrig ist, da sich im Unionsrecht hierfür keine Rechtsgrundlage findet.[24]

Zu 8:
Datenschutz, § 5 Abs. 1, § 6 und § 2 Abs. 1 Satz 3 SächsEGovG

Fragen zum Datenschutz sind im Evaluierungsbericht nur in folgendem Umfang angesprochen: § 5 Abs. 1 SächsEGovG verpflichtet Behörden zur Erstellung von Datenschutz- und Informationssicherheitskonzepten. § 6 SächsEGovG regelt die Einrichtung gemeinsamer Verfahren, die eine gleichmäßige datenschutzkonforme Rechtsanwendung sicherstellen soll. § 2 Abs. 1 Satz 3 SächsEGovG verpflichtet staatliche Behörden und Träger der Selbstverwaltung für die elektronische Kommunikation Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden. Dazu wurde bereits unter Punkt 1 Stellung genommen.

Insbesondere der Umfang der Erstellung von Datenschutz- und Informationssicherheitskonzepten nach § 5 Abs. 1 SächsEGovG ist laut Evaluierungsbericht bisher noch nicht in ausreichendem Maß vorangeschritten. Nur ¾ der befragten Behörden gaben an, eine oder mehrere solcher Maßnahmen bereits durchgeführt zu haben. An der Befragung teilgenommen haben jedoch nur 15 % der sächsischen Behörden. Als entsprechende Maßnahmen wurden genannt: Erstellung und Aktualisierung von IT-Sicherheitskonzepten und Handlungsrichtlinien, Bestellung eines Datenschutzbeauftragten und Umsetzung von Maßnahmen des Sächsischen Datenschutzgesetzes. Es ist davon auszugehen, dass hier noch zusätzlicher Handlungsbedarf besteht, um Schutzlücken zu schließen und die informationelle Selbstbestimmung der Verwaltungskunden zu gewährleisten.

In diesem Zusammenhang ist insbesondere auf die Notwendigkeit der Benennung eines behördlichen Datenschutzbeauftragten hinzuweisen. Die Bestellung eines behördlichen Datenschutzbeauftragten ist eine Maßnahme im Rahmen der Erstellung von Datenschutz- und Informationssicherheitskonzepten nach § 5 Abs. 1 SächsEGovG. Bisher bestand nach § 11 Abs. 1 Satz 1 SächsDSG keine Pflicht dazu („können“). Nach Art. 37 Abs. 1 lit. a DSGVO wird mit Geltung der Verordnung am 25. Mai 2018 jedoch die Pflicht bestehen, einen Datenschutzbeauftragten zu benennen, wenn „die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird […]“. Da der Entwurf des Sächsischen Datenschutz-Anpassungsgesetzes[25] keine Regelungen bezüglich der Benennung behördlicher Datenschutzbeauftragter vorsieht, sondern lediglich Regelungen zum Sächsischen Datenschutzbeauftragten als Aufsichtsbehörde im Sinne des Art. 51 ff. DSGVO, gilt Art. 37 DSGVO unmittelbar.

Da die Vorgaben der Datenschutz-Grundverordnung einen beachtlichen Aufwand für die Datenschutzbeauftragten bedeuten werden,[26] ist dringend anzuraten, die personellen Ressourcen entsprechend aufzustocken, um den Anforderungen der zukünftigen Rechtslage gerecht zu werden.

---

24 *Nebel*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Baden-Baden 2018, § 3 Rn. 124.

25 Entwurf eines Sächsischen Datenschutz-Anpassungsgesetzes vom 29. September 2017, SLT-Drs. 6/10918.

26 Vgl. hierzu auch die Untersuchung vom Januar 2017 zum zusätzlichen Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung von *Roßnagel*, abrufbar unter http://suche.transparenz.hamburg.de/dataset/gutachten-zum-zusaetzlichen-arbeitsaufwand-fuer-die-aufsichtsbehoerden-der-laender-durch-d-2017.

Die Bestimmungen des Sächsischen Datenschutzgesetzes aus dem Jahr 2003 bleiben nach § 5 Abs. 2 SächsEGovG unberührt. Mit der Anpassung des Datenschutzgesetzes an die Datenschutz-Grundverordnung wurde begonnen.[27] Dieses ist im Übrigen aber nicht Gegenstand der vorliegenden Evaluierung.

Zu 9: Informationssicherheit

Zu 9.1: Allgemeine Informationssicherheit, § 9 Abs. 2 und § 13 Abs. 2 SächsEGovG

§ 9 Abs. 2 SächsEGovG verpflichtet staatliche Behörden zu angemessenen organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen zur Einhaltung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz für die in ihren informationstechnischen Systemen verarbeiteten Daten. § 13 Abs. 2 SächsEGovG verpflichtet die Träger der Selbstverwaltung zur Einhaltung der Beschlüsse des IT-Planungsrats zur IT-Sicherheit.

Grundlegende Maßnahmen zur Informationssicherheit wurden bereits vor Inkrafttreten des Sächsischen E-Government-Gesetzes angestoßen. Hierzu gehört etwa die Verwaltungsvorschrift Informationssicherheit, die Strategien und Organisationsstrukturen regelt, die für die Etablierung der Informationssicherheit in der Staatsverwaltung erforderlich sind. Der Handlungsleitfaden zum Sächsischen E-Government-Gesetz benennt wesentliche technische Vorkehrungen, die auch die Träger der Selbstverwaltung ansprechen. Der Evaluierungsbericht legt offen, dass nur etwas mehr als die Hälfte der staatlichen Behörden und weniger als die Hälfte der Träger der Selbstverwaltung grundlegende Maßnahmen umgesetzt haben und dass die Implementierung der entsprechenden Maßnahmen stagniert. Daraus ist zu schließen, dass die Vorgaben und Empfehlungen der Verwaltungsvorschrift nicht mehr in ausreichendem Maße Wirkung entfalten.

Die Vorgaben und Empfehlungen der verschiedenen Rechtsgrundlagen und darauf basierenden Handlungsleitfäden und angestoßenen Arbeitskreise sind durchaus umfangreich und vielfältig. Für eine einheitliche Implementierung der Informationssicherheit ist anzuraten, diese vielfältigen Kataloge zu vereinheitlichen und – da der Stand der Informationssicherheit mehrheitlich auf Vorgaben von vor Inkrafttreten des Sächsischen E-Government-Gesetzes beruht – gegebenenfalls an die aktuellen Vorgaben insbesondere des BSI anzugleichen.

Nach Wirksamwerden der Datenschutz-Grundverordnung sind zudem deren Vorgaben zur Informationssicherheit zu beachten. Nach Art. 32 DSGVO sind technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit der Verarbeitung personenbezogener Daten sicherzustellen.[28] Die in Art. 32 Abs. 1 DSGVO genannten Maßnahmen der Pseudonymisierung, Verschlüsselung, Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit und anderen sind nicht abschließend, so dass jeder Verantwortliche gegebenenfalls weitere Maßnahmen ergreifen muss. Dies erfordert eine umfassende Prüfung des jeweiligen Datenverarbeitungssystems, eventuell einschließlich einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.[29]

Darüber hinaus sollte sich darauf konzentriert werden, die Vorgaben und Empfehlungen der verschiedenen – verordnungskonformen – Rechtsgrundlagen, Handlungsleitfäden und Arbeitskreise praktisch umzusetzen. Entscheidend hierfür ist es, die personellen Ressourcen zu stärken. Nur so entstehen in den einzelnen Behörden und Selbstverwaltungseinheiten Kapazitäten, um sich um die

---

27 Entwurf eines Sächsischen Datenschutz-Anpassungsgesetzes vom 29. September 2017, SLT-Drs. 6/10918.

28 *Husemann*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Baden-Baden 2018, § 5 Rn. 133 ff.

29 Dazu im Einzelnen *Friedewald u. a.,* White Paper Datenschutz-Folgenabschätzung, hrsg. von Forum Privatheit, 3. Aufl. 2017, www.forum-privatheit.de, im Erscheinen.

wirkungsvolle Umsetzung der Informationssicherheitsleitlinien zu kümmern. Zumindest sollte in jeder Behörde und bei jedem Träger der Selbstverwaltung ein Beauftragter für Informationssicherheit zur Verfügung stehen. Dies ist bisher nur vereinzelt der Fall. Dabei wirkt jede, auch nur geringfügige personelle Verbesserung als Multiplikator, um insbesondere durch regelmäßige Schulungen und Sensibilisierung der Mitarbeiter eine dauerhafte Steigerung der organisatorischen Maßnahmen zu erreichen. Es sollte eine Verpflichtung im Gesetz verankert werden, Beauftragte für die Informationssicherheit zu benennen, um diese gegebenenfalls vollstreckbar zu machen.

Zu 9.2 Informationssicherheit – Kommunikationsnetze, § 11 und § 15 SächsEGovG

§§ 11 und 15 SächsEGovG regeln die elektronische Datenübermittlung in einem informationstechnischen Netz (Sächsisches Verwaltungsnetz, SVN) sowohl zwischen staatlichen Behörden untereinander als auch zwischen staatlichen Behörden und Trägern der Selbstverwaltung. Die Vorschriften dienen in erster Linie der Gewährleistung der Informationssicherheit. Der Nutzungsgrad ist laut Evaluierungsbericht hoch, hat sich aber durch die Einführung des Sächsischen E-Government-Gesetzes nicht weiter erhöht. Die von der Staatsregierung vorgeschlagene Schlussfolgerung, die Träger der Selbstverwaltung zur Nutzung des SVN zu verpflichten – zumindest für bestimmte zentrale Dienste – geht jedoch fehl, da die Vorschriften eine Pflicht zur Nutzung bereits hinreichend deutlich machen. Vielmehr ist der Fokus verstärkt auf die Versorgung ländlicher Gebiete mit Breitbandanschlüssen zu legen, um die essentielle Voraussetzung der Nutzung des SVN zu schaffen.

Zu 10:
Barrierefreiheit, § 7 und § 12 Abs. 6 SächsEGovG

Die Umsetzung der Barrierefreiheit vor allem im kommunalen Bereich ist nach den Ausführungen des Evaluierungsberichts alarmierend. Die UN-Behindertenrechtskonvention ist seit dem Jahr 2008 in Kraft und seit dem Jahr 2009 in Deutschland ratifiziert. Staatliche Behörden und Träger der Selbstverwaltung sind dazu verpflichtet, elektronische Kommunikation und elektronische Dokumente nach § 7 SächsEGovG und Verfahren zur elektronischen Vorgangsbearbeitung und Aktenführung nach § 12 Abs. 6 SächsEGovG so zu gestalten, dass sie auch von Menschen mit Behinderung grundsätzlich genutzt werden können. Um die Barrierefreiheit effektiv umzusetzen, sollte der Gesetzeswortlaut die Verpflichtung zur Umsetzung der Konvention deutlicher unterstreichen. Es ist mindestens das Wort „grundsätzlich“ in § 7 und § 12 Abs. 6 SächsEGovG zu streichen, da dies Ausnahmen impliziert, wo keine zulässig sind. Außerdem sollte § 7 SächsEGovG nicht auf § 3 Sächsisches Integrationsgesetz (Barrierefreiheit baulicher Anlagen, Verkehrsmittel etc.) verweisen, sondern auf dessen § 7, da dieser für Informationstechnik spezieller ist.

Zu 11:
Experimentierklausel, § 20 SächsEGovG

Die Experimentierklausel dient der vereinfachten Erprobung und Weiterentwicklung von E-Government-Anwendungen durch sachlich und räumlich begrenzte, befristeter Ausnahmen von der Anwendung verschiedener landesrechtlicher Verfahrens- und Zuständigkeitsvorschriften. Diese Vorschrift ist sehr zu begrüßen, ermöglicht sie doch die Einführung, Anwendung und Erprobung verschiedener E-Government-Maßnahmen in einem realen Umfeld. Dies ist zudem geeignet, die Akzeptanz entsprechender technischer Lösungen bei Behörden und Bürgerinnen und Bürgern zu fördern und zu testen.

Von der Experimentierklausel wurde seit Inkrafttreten des Gesetzes kein Gebrauch gemacht. Es ist zu vermuten, dass dies mit dem umfangreichen Genehmigungsprozess zusammenhängt, da entsprechende Ausnahmevorschriften nur für einzelne Behörden und durch die zuständige oberste Staatsbehörde nur im Benehmen mit den Beauftragten für Informationstechnologie des Freistaates Sachsen und nach Zustimmung des Staatsministeriums des Innern bzw. im Einvernehmen mit dem Staatsministerium der Finanzen erlassen werden können.

Im Interesse einer zügigen Weiterentwicklung des E-Government ist anzuraten, diese Genehmigungsvoraussetzungen stark zu reduzieren. Auch wäre es sinnvoll, entsprechende Ausnahmen nicht nur für einzelne Behörden zuzulassen, sondern diese auf breiter Basis zugänglich zu machen. Hierzu könnte etwa ein gemeinsames Gremium mit Vertretern aller obersten Staatbehörden eingerichtet werden, um gemeinsam zu eruieren, wo Ausnahmevorschriften sinnvoll sind, um E-Government-Anwendungen frühzeitig in der Praxis zu testen.

Fazit

Das Sächsische E-Government-Gesetz ist durchaus geeignet, eine medienbruchfreie elektronische Verwaltung zu etablieren. Neben einigen geringfügigen gesetzgeberischen Klarstellungen ist der Fokus aber vor allem auf den Abbau der finanziellen Hürden und den Ausbau der personellen Ressourcen zu legen, die eine wichtige Anschubwirkung haben, um E-Government-Anwendungen weiter zu verbreiten, Datenschutz und Informationssicherheit zu leben, Mitarbeiter zu sensibilisieren und die Akzeptanz für die elektronische Verwaltung sowohl innerhalb der Behörden als auch bei Bürgerinnen und Bürgern zu steigern.

Ass. iur. Maxi Nebel