Veranstaltung der Landesfachkommission (LFK) Kultur und Medien des Wirtschaftsrates der CDU e.V am 10. September 2014 in Magdeburg zum Thema: **„**Sichere und rechtsverbindliche Kommunikation zwischen Wirtschaft und Verwaltung?!“

Datenschutzrechtliche und technisch-organisatorische Anforderungen an eine moderne Kommunikation zwischen Wirtschaft und Verwaltung

(Landesbeauftragter für den Datenschutz, Dr. Harald von Bose)

Einführung

Informations- und Kommunikationstechnologien (IKT) sind für die heutige Gesellschaft, die Wirtschaft sowie die öffentliche Verwaltung von erheblicher Bedeutung. Wachstum und Wettbewerbsfähigkeit der modernen Wirtschaft, aber auch eine innovative und effiziente Verwaltung sind ohne Einsatz dieser Schlüsseltechnologien nicht mehr vorstellbar.
Beispiele hierfür sind u.a. Mobile Computing, Social Media, Cloud-Dienste, Internet of everything (Industrie 4.0.), Big Data.

- vgl. auch Digitale Agenda 2014-2017 (vom 20. August 2014)

- zu beachten: aber auch in Deutschland derzeit 20% der Bevölkerung ohne Internetzugang!

Unter Electronic Government (E-Government) versteht man nach der Speyerer Definition die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien.

Mit der Bereitstellung von E-Government-Verfahren durch die Verwaltung sollen den Bürgerinnen und Bürgern sowie den Unternehmen langfristig neue und vereinfachte Möglichkeiten der Informationsbeschaffung, Kommunikation und Antragstellung über das Internet zur Verfügung stehen. E-Government ist gleichzeitig die Voraussetzung für Open Government.

Der IT-Planungsrat hat bereits auf seiner 3. Sitzung am 24. September 2010 die Nationale E-Government Strategie (NEGS) beschlossen. Sie bildet damit eine gemeinsame Strategie von Bund, Ländern und Kommunen im Rahmen der E-Government-Aktivitäten in Deutschland. Drei der sechs definierten Zielbereiche der NEGS betreffen explizit die Themen Nutzen für Bürger, Unternehmen und Verwaltung, Datenschutz, Datensicherheit, Transparenz und Gesellschaftliche Teilhabe bzw. Informationsfreiheit. Mit diesen Themen beschäftigt sich der Landesbeauftragte bereits seit 2003 und seit dem 22. März 2012 auch die Enquete-

Kommission des Landtages Sachsen-Anhalts unter dem Thema „Öffentliche Verwaltung konsequent voranbringen – bürgernah und zukunftsfähig gestalten“.

Datenschutz ist *Grundrechtsschutz.*

Die Grundrechte auf freie Entfaltung der Persönlichkeit sowie auf Unantastbarkeit der Menschenwürde schützen gegen unbegrenzte Erhebung, Verarbeitung und Nutzung der persönlichen Daten.

Das *allgemeine Persönlichkeitsrecht* (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst *neben* dem „**Recht auf informationelle Selbstbestimmung**“ nach dem Urteil vom 15. Dezember 1983 (BVerfGE 65, 1; 1 BvR 209, 269, 362, 420, 440, 484/83) gemäß dem Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) zur sog. „Online-Durchsuchung“ auch das „**Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**“.

Die *Verfassung* des Landes Sachsen-Anhalt gewährt in Art. 6 Abs. 1 ebenfalls diesen Schutz der Persönlichkeit.

Artikel 6 Datenschutz, Umweltdaten:

(1) Jeder hat das Recht auf Schutz seiner personenbezogenen Daten. In dieses Recht darf nur durch oder auf Grund eines Gesetzes eingegriffen werden. Dabei sind insbesondere Inhalt, Zweck und Ausmaß der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten zu bestimmen und das Recht auf Auskunft, Löschung und Berichtigung näher zu regeln.

Das *Datenschutzgesetz Sachsen-Anhalt (**DSG LSA**)* legt für *öffentliche Stellen des Landes* und deren *Auftragnehmer*, insbesondere für die automatisierte Verarbeitung personenbezogener Daten, technologieunabhängige *Sicherheitsziele* fest, welche durch die konkrete Umsetzung von technischen und organisatorischen Maßnahmen entsprechend erfüllt werden müssen.

Die **Datensicherheit** bei der automatisierten Verarbeitung personenbezogener Daten muss durch eine entsprechende Umsetzung der Sicherheitsziele des § 6 Abs. 2 DSG LSA *(Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz)* durch *jede* öffentliche Stelle gewährleistet werden.

Elektronische Kommunikation zwischen Wirtschaft und Verwaltung wird also aus datenschutzrechtlicher Sicht nach der Umsetzung dieser Sicherheitsziele des § 6 Abs. 2 DSG LSA zu beurteilen sein. Im Fokus stehen hier die ***Vertraulichkeit***, ***Integrität*** und die ***Authentizität*** bei der elektronischen Kommunikation.

Frage:

Wie sieht nun allerdings die Praxis *vier* Jahre nach Beschluss dieser NEGS aus?

Nach einer Online-Umfrage zur Nutzung von E-Government-Angeboten durch die Wirtschaft des Beratungsunternehmens Bearingpoint zusammen mit dem Deutschen Industrie- und Handelskammertag e. V.(DIHK) im April bis Mai 2014 unter deutschen Unternehmen war das Ergebnis allerdings erschreckend. Legen die Ergebnisse der Umfrage doch den Schluss nahe, dass die E-Government-Angebote oft kaum einen Nutzen bringen:

Die große Mehrheit der Unternehmen (**77%**) hat Bedenken hinsichtlich *Datenschutz* und *Sicherheit* und nutzt daher das digitale Angebot der Verwaltung nicht oder nicht in vollem Umfang. Damit führt fehlendes Vertrauen zu fehlender Akzeptanz.

- *2 Bitkom-Umfragen: Deutschland im E-Government auf dem Niveau von Griechenland!*
- *Die allermeisten der Unternehmen kommunizieren nicht verschlüsselt; aus Unkenntnis oder weil der Kommunikationspartner nicht verschlüsselt*

Das Ergebnis dieser Umfragen und auch die Einschätzung der Unternehmen sind nicht ganz unberechtigt. Für Sachsen-Anhalt dürfte diese Einschätzung auch zutreffen. Das ist auch die Folge eines Vollzugs- und Umsetzungsdefizits trotz bestehender rechtlichen Rahmenbedingungen und den kaum vorhandenen E-Government-Anwendungen für die Bürgerinnen und Bürger sowie für die Wirtschaft. Bereits in meiner Stellungnahme bei der Anhörung vor der Enquete-Kommission des Landtages Sachsen-Anhalts zum Thema „E-Government-Strategie“ habe ich mich dazu kritisch geäußert. E-Government benötigt Vertrauen, Verantwortung und Verlässlichkeit; jedoch gibt es gravierende Widersprüche:

„Die meisten Internetnutzer haben angeblich – bei freundlichem Desinteresse am Datenschutz – nichts zu verbergen. Die Wirtschaft und die Machtmonopole des Internets beanspruchen die Datenprofile für sich. Der Staat verweist auf die Datenmissbräuche dieser Akteure, fordert vom überforderten einzelnen Menschen mehr Selbstdatenschutz, um zugleich als Präventionsstaat zugunsten von totaler Sicherheit selbst Big Data zu betreiben,

und dann scheinfreundlich den Bürger zur Nutzung von Angeboten des E-Government zu animieren“ (XI. Tätigkeitsbericht zum Datenschutz, Nr. 1).

I. Was sind nun die wesentlichen rechtlichen Rahmenbedingungen?

1. Verwaltungsverfahrensgesetz und E-Government-Gesetz (Bund)

1.1 Verwaltungsverfahrensgesetz

Das **Verwaltungsverfahrensgesetz** des Bundes (VwVfG), welches aufgrund der Verweisung in **§ 1 Abs. 1** des Verwaltungsverfahrensgesetz Sachsen-Anhalt (VwVfG LSA) Landesverwaltungsverfahrensgesetzes auch für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des **Landes** und der seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts gilt, sieht **bereits ab dem 1. Februar 2003 die Möglichkeit der elektronischen Kommunikation vor**. Nach **§ 3a Abs. 1 VwVfG** ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet (hat). Diese Zugangseröffnung kann ausdrücklich oder konkludent erfolgen. So ist z. B. die Angabe einer E-Mail-Anschrift als Kontakt- und Kommunikationsanschrift ausreichend.

Nach **§ 3a Abs. 2 VwVfG** ist die Ersetzung der Schriftform durch die elektronische Form möglich. In diesen Fall muss das elektronische Dokument mit einer *qualifizierten elektronischen Signatur (QES)* nach dem *Signaturgesetz* versehen sein.

Das **Signaturgesetz** (SigG) unterscheidet **4 Typen** von Signaturen, nämlich der einfachen, fortgeschrittenen, qualifizierten und qualifizierten elektronischer Signatur mit Anbieterakkreditierung. Die einfache und fortgeschrittene Signatur ersetzen die Schriftform nicht (vgl. dazu auch § 126a BGB für das Zivilrecht).

Im Einzelnen sind nach § 2 SigG:
1. "*elektronische Signaturen*" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. "*fortgeschrittene elektronische Signaturen*" elektronischen Signaturen nach Nr. 1, die
   a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
   b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
   c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und

d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

3. "*qualifizierte elektronische Signaturen*" elektronische Signaturen nach Nr. 2, die
   a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
   b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Eine **qualifizierte elektronische Signatur (QES)** muss also zusätzlich zur fortgeschrittenen Signatur auf einem vom Zertifizierungsdienste-Anbieter (Trust-Center) zum Zeitpunkt der Erstellung ausgestellten, gültigen Zertifikat beruhen, welches eindeutig einer *natürlichen* Person zugeordnet ist und mit einer sicheren Signaturerstellungseinheit (zumeist einer Chipkarte) erzeugt worden ist.
D.h. zur Erzeugung einer QES werden eine Chipkarte (mit darauf gespeicherten Zertifikaten), ein entsprechendes sicheres Kartenlesegerät und Zertifizierungssoftware benötigt.
Das Zertifikat kann auch zur *Verschlüsselung* eingesetzt werden.

Bei einer gültigen QES wird die **Echtheit** der Urkunde inklusive der **Identität** des Erklärenden (des Signaturschlüssel-Inhabers) **vermutet** (§ 173 VwGO i.V. m. **§ 371a ZPO**).

4. Um eine *qualifizierte elektronische Signatur mit Anbieterakkreditierung* handelt es, wenn der Zertifizierungsdienste-Anbieter (Trust-Center) den Nachweis der technischen und administrativ-organisatorischen Sicherheit gegenüber der Bundesnetzagentur erbracht hat und akkreditiert wurde. Das ist bei den meisten in Deutschland ansässigen Zertifizierungsdienste-Anbietern der Fall.

Zusatzhinweis:
Mit der **Verordnung** des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 16. Juli 2014 (2012/0146 (COD)) werden auch gesonderte Regelungen für natürliche und *juristische* Personen geschaffen. Die Verordnung gilt ab 1. Juli 2016. Sie legt die Bedingungen fest, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel für natürliche und juristische Personen, die einem *notifizierten* elektronischen Identifizierungssystem eines anderen Mitgliedstaates unterliegen, anerkennen. Die notifizierten elektronischen Identifizierungssysteme werden nach Art. 8 Abs. 1 der Verordnung in die Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ eingeteilt. Bis Juli 2015 muss die Kommission im Wege von

Durchführungsrechtsakten technische Spezifikationen, Normen und Verfahren mit Mindestanforderungen festlegen. Nach Artikel 46 der Verordnung darf einem *elektronischen* Dokument die Rechtswirkung und die Zulässigkeit als Beweismittel in einem Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt. Die Verordnung berührt nicht das nationale Recht, d.h. das Signaturgesetz und die Signaturverordnung bleiben gültig, sollen aber nach Verlautbarung des Bundeswirtschaftsministeriums angepasst werden.

1.2 E-Government-Gesetz des Bundes (EGovG)

Mit dem Gesetz zur Förderung der elektronischen Verwaltung (**E-Government-Gesetz - EGovG**) vom 25. Juli 2013 (BGBl. I S. 2749) wurden die Möglichkeiten der elektronischen Kommunikation des § 3a Abs. 2 VwVfG erweitert. Hintergrund ist die Tatsache, dass die bereits seit vielen Jahren verfügbare QES bisher in der Verwaltungspraxis noch keinen Durchbruch erzielen konnte.

Nach **§ 3a Abs. 2 Satz 4 VwVfG** kann jetzt die **Schriftform** auch ersetzt werden:

1. durch unmittelbare Abgabe der Erklärung in einem **elektronischen Formular**, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der **Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes**;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der **Behörden** durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4. durch **sonstige sichere Verfahren**, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

Nach **§ 2 Abs. 1 EGovG** ist nunmehr jede Behörde ab dem **1. Juli 2014** verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente zu eröffnen, auch soweit sie mit einer *qualifizierten elektronischen Signatur* versehen sind. Dies gilt also auch für Landes- und Kommunalbehörden, die Bundesrecht ausführen.

Bundesbehörden werden darüber hinaus verpflichtet auch einen De-Mail-Zugang und zur Identifizierung einer Person den elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anzubieten. Für Landes-und Kommunalbehörden besteht diese Verpflichtung bisher nicht.

Weiterhin sollen die Behörden des Bundes gemäß **§ 6 EGovG** ab 2020 die Akten elektronisch führen. Der Bundesgesetzgeber veranschlagt damit eine Vorlaufzeit bis zur elektronischen Aktenführung von sechs Jahren.
Die Einführung der **elektronischen Akte** ist damit eine wesentliche Grundvoraussetzung für Open Government und Open Data. Deshalb verlangt auch der § 12 EGovG die Verwendung maschinenlesbarer Formate, damit eine automatisierte Weiterverarbeitung mittels Software ermöglich wird und dadurch Medienbrüche vermieden werden.

2. Abgrenzung zwischen QES und Identitätsnachweis (nPA) und De-Mail-Nutzung

2.1 Identitätsnachweis – eID (nPA)

Der Schriftformersatz nach § 3a Abs. 2 Satz 4 Nr. 1 (Formular) und 4 (anderes sicheres Verfahren) VwVfG ist mit dem **elektronischen Identitätsnachweis** nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes verbunden. Dieser Identitätsnachweis ist aber nicht mit der QES gleichzusetzen, denn er ermöglicht nur die Feststellung der Identität einer natürlichen Person (*Authentizität*). Er ermöglicht keine Überprüfung der Integrität (Unversehrtheit und Vollständigkeit) eines Dokumentes. Es ist also nicht feststellbar, ob die Daten unverändert und vollständig übermittelt wurden.

2.2 De-Mail-Nutzung

Mit dem am 3. Mai 2011 in Kraft getreten **De-Mail-Gesetz** sollen Nachrichten und ihr Inhalt stärker geschützt werden als bei herkömmlichen E-Mails. De-Mail-Dienste sind nach § 1 Abs. 1 De-Mail-Gesetz Telekommunikationsdienste auf einer elektronischen Plattform, die eine sichere, vertrauliche und nachweisbare Kommunikation für jedermann im Internet gewährleisten sollen.

Der Weg vom Versender zum Empfänger ist nur transportverschlüsselt. Zwar ist die Nachricht auf dem Weg zwischen dem De-Mail-Diensteanbieter (DMDA) des Versenders und dem DMDA des Empfängers auch zusätzlich inhaltsverschlüsselt. Allerdings verpflichtet § 3 Abs. 4 Nr. 4 De-Mail-Gesetz den DMDA, die De-Mail auf Befall mit Schadsoftware zu überprüfen, d.h. die Inhaltverschlüsselung muss deshalb aufgehoben werden. Dieser Prüfprozess erfolgt zwar automatisiert auf Servern in einem Rechenzentrum des DMDA, das den Vorgaben des BSI entspricht. Gleichwohl besteht ein Restrisiko, dass insbesondere Administratoren des Anbieters vom Nachrichteninhalt Kenntnis nehmen können. Die bloße Transportverschlüsselung führt im Ergebnis dazu, dass der Inhalt der De-Mail¸ im Unterschied zu einer Ende-zu-Ende-Verschlüsselung mittels QES, unverschlüsselt im Postfach des Empfängers abgelegt wird.

Für den DMDA ergeben sich aus dem De-Mail-Gesetz keine Pflichten für eine Ende-zu-Ende-Verschlüsselung vom Versender bis zum Empfänger. Er darf den Versand Ende-zu-Ende-verschlüsselter Nachrichten lediglich nicht verhindern. Im Gegensatz zu einer Ende-zu-Ende-Verschlüsselung mittels QES stellt die De-Mail keine durchgängige Verschlüsselung zwischen Versender und Empfänger dar und bietet sich daher aus datenschutzrechtlicher Sicht für eine Versendung besonders schutzbedürftiger Daten (wie z. B. Sozialdaten) nicht an.

Zusammenfassend ist aus datenschutzrechtlicher Sicht festzustellen, dass mittels De-Mail die *Authentizität* des Versenders sichergestellt werden kann. Die *Integrität* der Daten zwar höher ist als bei einer herkömmlichen E-Mail, wegen der **Manipulationsmöglichkeit** beim De-Mail-Diensteanbieter aber eben nicht sicher gewährleistet werden kann.

Bereits im Jahr 2009 hat die Datenschutzkonferenz für diese Kommunikation die standardmäßige Ende-zu-Ende-Verschlüsselung zwischen Versender und Empfänger gefordert.

Mittlerweile gibt es Überlegungen des Bundesministeriums für Verbraucherschutz die Ende-zu-Ende-Verschlüsselung bei E-Mail-Diensten gesetzlich vorzuschreiben. Auch will sich die Bundesregierung dafür einsetzen, dass ein solcher Passus in die geplante **EU-Datenschutz-Grundverordnung** aufgenommen wird (Datenschutz durch **privacy by design**). Darüber hinaus plant die Bundesregierung Presseberichten des Spiegel zufolge in den kommenden drei Jahren mindestens 250 Mio € für den Ausbau einer abhör-

sicheren Behördenkommunikation einzusetzen. Inwieweit davon auch Landes- und Kommunalbehörden partizipieren werden, ist bisher nicht bekannt.

Nach **§ 3 des IT-NetzG** muss der Datenaustausch zwischen dem Bund und den Ländern ab dem 1. Januar 2015 über das **Verbindungsnetz** erfolgen. Inwieweit diese geplanten Investitionen im Zusammenhang mit dem Aufbau eines solchen abhörsicheren Netzes stehen, ist ebenfalls bisher nicht bekannt.

3. Vertraulichkeit bei der elektronischen Kommunikation

Aus datenschutzrechtlicher Sicht setzt die *Vertraulichkeit* voraus, dass bei der elektronischen Kommunikation von personenbezogenen Daten nur Befugte Kenntnis erhalten (§ 6 Abs. 2 Nr.1 DSG LSA). Der Schutz der Vertraulichkeit kann durch eine **Ende-zu-Ende-Verschlüsselung** gewährleistet werden. Eine entsprechende Verpflichtung zur Verschlüsselung ist weder im Verwaltungsverfahrensgesetz noch im EGovG explizit geregelt.

Nach dem **Beschluss des Bundesgerichtshofes** vom 26. Februar 2013 (Az.: KVZ 57/12) kann ein Unternehmen von einer Behörde nicht verpflichtet werden, über eine ungesicherte E-Mail-Verbindung unternehmensinterne Daten zu übermitteln. Da seit dem 1. Juli 2014 gemäß § 2 Abs. 1 EGovG ein Zugang für die Übermittlung elektronischer Dokumente eröffnet werden muss, dürfte seit dem auch ein Anspruch auf eine verschlüsselte elektronische Kommunikation bestehen (so auch die Literatur, vgl. etwa Schmitz in: Stelkens/Bonk/Sachs, VwVfG, 8. Auflage 2014, § 3a Rn. 14).

Als erstes Bundesland hat der Freistaat Sachsen im **Sächsischen E-Government-Gesetz** (SächsEGovG) vom 9. Juli 2014 (Sächsisches GVBl. S. 398) für die elektronische Kommunikation die Anwendung entsprechender Verschlüsselungsverfahren grundsätzlich vorgeschrieben.

4. Datenschutzrechtliche Schlussfolgerungen

Nach **§ 2 Abs. 1 EGovG** ist **jede** Behörde verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen. Doch was für einen Nutzen hat die elektronische Kommunikation für beide Seiten, wenn die Behörde keine elektronische Aktenführung hat und das Dokument dann doch wieder ausdrucken und in die Papierakte geben muss? Unternehmen haben nach § 2 Abs. 1 EGovG sowie der Rechtsprechung des BGH einen Anspruch auf eine verschlüsselte Kommunikation. Doch was nützt dem Unternehmen die verschlüsselte Kommunikation mit der Behörde, wenn die Behörden untereinander im Landesnetz unverschlüsselt kommunizieren, so dass ein Angreifer hier

jederzeit weitergegebene Unternehmensdaten, insbesondere Betriebs- und Geschäftsgeheimnisse, abfangen kann? Man denke hier nur an den NSA-Skandal oder an die Möglichkeiten der Wirtschaftsspionage.

Daher ist aus **datenschutzrechtlicher Sicht** mindestens eine vertrauliche (verschlüsselte) Kommunikation zwischen Unternehmen und Behörde, praxistaugliche Verfahren, welche die Integrität der Daten und Authentizität der Kommunikationspartner gewährleisten, eine elektronische Aktenführung in der öffentlichen Verwaltung sowie ein sicheres Landesnetz erforderlich.

II. Was hat sich in Sachsen-Anhalt getan?

Vorbemerkung:

Die Landesregierung hatte bereits am 29. April 2003 mit dem Beschluss eines E-Government-Grundkonzepts und dem E-Government-Aktionsplan für die Landesverwaltung 2004 – 2010 die strategischen Rahmenbedingungen für die Einführung elektronischer Verwaltung geschaffen. Seitens der Ressorts wurden im Rahmen der E-Government-Maßnahmenpläne 2005-2006, 2007 und 2008-2009 entsprechende Leitprojekte und Basiskomponenten umgesetzt. Diese Leitprojekte resultierten im Wesentlichen zum einen aus der Beteiligung des Landes an den E-Government-Projekten des Bundes (DOL – Deutschland Online) und zum anderen aus Bund-Länder-Fachverfahren.

Besonders mit den Basiskomponenten für das E-Government (wie u. a. dem Landesportal als Dienstleistungsportal, dem dazugehörigen Content Management System, dem Formularserver, der Virtuellen Poststelle und dem Geodatenserver) wurden grundlegende Voraussetzungen für die Möglichkeit zur elektronischen Kommunikation der Bürgerinnen und Bürger sowie der Wirtschaft mit der Verwaltung geschaffen. Hierzu gehören beispielhaft solche Verfahren wie die Umsetzung der EU-Dienstleistungsrichtlinie mittels eines Einheitlichen Ansprechpartners, des Leistungskataloges (LeiKa), des Behördenfinders Deutschland (BFD) und des Föderalen Informationsmanagements (FIM) oder der Initiative D 115. Bei allen Anstrengungen zur weiteren Forcierung von E-Government-Vorhaben wurde der **sicheren** und **rechtsverbindlichen Kommunikation** aber aus datenschutzrechtlicher Sicht nicht die notwendige Aufmerksamkeit geschenkt.

1. Public Key Infrastructure (**PKI LSA**) Sachsen-Anhalt

   Bereits im Jahr 2006 wurden mit dem Aufbau einer Public Key Infrastructure (**PKI LSA**) Sachsen-Anhalt die Voraussetzungen zur Anwendung von fortgeschrittenen und qualifizierten Signaturen sowie der Verschlüsselungsmöglichkeit der elektronischen Kommunikation geschaffen (Organisation und Aufgaben der Sicherheitsinfrastruktur, RdErl. MF vom 14.11.2011, MBl. LSA S. 532; Bezug: RdErl. des MI vom 14.03.2006, MBl. LSA S. 233). Ein flächendeckender Einsatz von fortgeschrittenen und qualifizierten Signaturen sowie der Verschlüsselungsmöglichkeit der elektronischen Kommunikation ist in Sachsen-Anhalt nicht erfolgt.
   Eine positive Ausnahme bildet z. B. das auch in Sachsen-Anhalt mit der Novellierung des Melderechtsrahmengesetzes seit dem1. Januar 2007 eingeführte nur noch elektronische bundesweite Rückmeldeverfahren zwischen den Meldebehörden bei Umzügen mittels Übermittlungsprotokoll OSCI-Transport (OSCI – Online Services Computer Interface).
   Mit dem Übermittlungsprotokoll OSCI-Transport werden die Anforderungen an Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit bei der elektronischen Übermittlung von Nachrichten im Internet gewährleistet.

2. **Einheitlicher Ansprechpartner** (EA) gem.§ 71a ff. VwVfG

   Nach der **EU-Dienstleistungsrichtlinie** (Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt) sollen sämtlich zur Aufnahme einer Dienstleistungstätigkeit im europäischen Binnenmarkt erforderlichen Verfahren und Formalitäten über eine besondere Kontaktstelle (dem „Einheitlichen Ansprechpartner“) erfolgen. In Umsetzung dieser Richtlinie wurde das VwVfG um die Regelungen zu diesem Einheitlichen Ansprechpartner ergänzt (§ 71a bis § 71e VwVfG). Für Unternehmen und Bürger im *Inland* wie auch im *europäischen Ausland* gilt das Verfahren gleichermaßen. **Auf Verlangen muss dieses Verfahren in elektronischer Form abgewickelt werden (§ 71e VwVfG)**. Die Vorschriften über die QES (§ 3a Abs. 2 Satz 2 und 3 VwVfG) sind anzuwenden.

   Mit der noch rechtzeitigen Verabschiedung des Gesetzes zur Umsetzung der europäischen Dienstleistungsrichtlinie in Sachsen-Anhalt vom 16. Dezember 2009 (GVBl. LSA S. 700) konnte die vorgegebene Umsetzungsfrist der EU-DLR bis zum 31. Dezember 2009 eingehalten werden. Nach § 10 des Einheitlicher-Ansprechpartner-Gesetzes (EAG LSA) ist das Landesverwaltungsamt seither der Einheitliche Ansprechpartner.

Dieses mit viel Aufwand entwickelte System wird aber nach meinem Kenntnisstand bis heute von deutschen und europäischen Unternehmen nur sehr zurückhaltend in Anspruch genommen. Eine Weiterentwicklung ist aber bis Ende 2015 geplant („**EA 2.0“**).

3. Verfahren zur Umsetzung der **eID-Funktion des nPA**

   Gegenwärtig sind dem Landesbeauftragten weder Pilotprojekte noch Verfahren zur Umsetzung der eID-Funktion des nPA bekannt.

4. **De-Mail**

   Überlegungen bzw. Konzepte zur Einführung und Nutzung von De-Mail-Diensten sind dem Landesbeauftragten nicht bekannt.

5. Strategie „Sachsen-Anhalt digital 2020

   Die **Strategie „Sachsen-Anhalt digital 2020“** vom 11. Oktober 2012 trifft keine grundlegenden Aussagen zur Einführung und Nutzung der QES, De-Mail und nPA für die Landesverwaltung. Gleiches gilt für eine Verschlüsselung der elektronischen Kommunikation der Verwaltung mit der Bevölkerung oder den Unternehmen.
   Die bisher fehlende Möglichkeit der Verschlüsselung stellt ein erhebliches Hindernis für die elektronische Verwaltungskommunikation dar (Bauer/ Heckmann/ Ruge/ Schallbruch/ Schulz, Verwaltungsverfahrensgesetz und E-Government, 2. Auflage, 2014, § 2 EGovG, Rn. 3).

   Im Rahmen eines Workshops mit dem zuständigen Ministerium der Finanzen im April 2014 wurde *keine* Anpassung bzw. Fortentwicklung dieser Strategie „Sachsen-Anhalt digital 2020“ (Informations- und Kommunikationstechnologie als Grundlage gesellschaftlicher Entwicklung und staatlicher Modernisierung) vom 11. Oktober 2012 in Aussicht gestellt. Obwohl dies gerade auch die Erkenntnisse aus dem NSA-Überwachungsskandal nahelegen.

   Lediglich der zur Strategie gehörende **Umsetzungsplan** sollte evaluiert bzw. in Abstimmung mit den Ressorts überarbeitet werden.

   Zumindest hat das Ministerium für Inneres und Sport sowie das Ministerium für Finanzen zu einem gemeinsamen **Workshop** von IMA-Org und IKT-Kreis am 19. September 2014 zum Thema „Folgerungen aus dem Gesetz zur Förderung der elektronischen Verwal-

tung sowie zur Änderung weiterer Vorschriften (EGovernment-Gesetz) für Sachsen-Anhalt“ eingeladen.

Mit Blick darauf, dass mit dem EGovG vom 25. Juli 2013 auch gleichzeitig der § 3a VwVfG an den Stand für eine moderne elektronische Kommunikation (**De-Mail, nPA**) angepasst wurde, hat damit das Land für eigene Umsetzung bereits ein Jahr ungenutzt verstreichen lassen.

6. **Dataport** als zentraler IT-Dienstleister der Landesverwaltung

Am 24. Februar 2014 trat der Staatsvertrag zwischen dem Land Schleswig-Holstein, der Freien und Hansestadt Hamburg, dem Land Mecklenburg-Vorpommern, der Freien Hansestadt Bremen, dem Land Niedersachsen und dem Land Sachsen-Anhalt über den Beitritt des Landes Sachsen-Anhalt zur rechtsfähigen Anstalt des öffentlichen Rechts „Dataport“ in Kraft, und das Land Sachsen-Anhalt als Trägerland trat damit rückwirkend zum 1. Januar 2013 dem IT-Verbund Dataport bei. Die Überleitung des Landesrechenzentrums an Dataport erfolgte zum 1. März 2014. Dataport ist ein Full Service Provider für Informationstechnik der Verwaltung. Aus datenschutzrechtlicher Sicht handelt es sich, auch wenn Sachsen-Anhalt eines der Trägerländer ist, um Auftragsdatenverarbeitung nach § 8 DSG LSA. Demzufolge wären z. B. Maßnahmen zur Datensicherheit (sichere Authentifizierung und Verschlüsselung) durch den Auftragnehmer Dataport umzusetzen. Die datenschutzrechtliche Verantwortung verbleibt jedoch bei den jeweiligen Ressorts.

Die Tätigkeit von Dataport als zentraler IT-Dienstleister der Landesverwaltung löst nicht die bereits erwähnten Regelungs- und Umsetzungsdefizite.

Es dürfte sich empfehlen, die einzelnen IKT-Strategien der mittlerweile sechs Dataport-Trägerländer *untereinander abzustimmen*. Insofern dürfte es für Sachsen-Anhalt nicht ausreichend sein, nur den *Umsetzungsplan* zur Strategie „Sachsen-Anhalt digital 2020“ zu evaluieren bzw. zu ergänzen.

III. Handlungsbedarf in Sachsen Anhalt

1. Praxis- und Vollzugsdefizite beseitigen!

   Es gibt gegenwärtig aus meiner Sicht ein *Praxis- und Vollzugsdefizit*, d. h. die Anwendung der QES hat sich in der Verwaltung noch nicht massenhaft durchgesetzt. Gleiches gilt für die Anwendung der neuen Vertrauensdienste wie nPA und De-Mail. Da es nunmehr um den Vollzug bestehender gesetzlicher Verpflichtungen geht, besteht akuter Handlungsbedarf, um diese Dienste anwenderfreundlich und kostengünstig zur Verfügung zu stellen.
   Der IT-Planungsrat hat diese grundsätzlichen Probleme bisher nicht aufgegriffen.

2. Verschlüsselung gesetzlich regeln!

   Eine verbindliche Regelung zur verschlüsselten elektronischen Kommunikation, wie in § 2 des Sächsischen E-Government-Gesetzes (SächsEGovG) vom 9. Juli 2014, existiert in Sachsen-Anhalt nicht (vgl. auch die Digitale Agenda 2014-2017 der Bundesregierung: „Deutschland soll Verschlüsselungsstandort Nr. 1 in der Welt werden.“).

3. Landes-E-Government-Regelung

   Für die Landesverwaltung gibt es bisher *keine* dem EGovG (des Bundes) entsprechenden Regelungen, wenn Landesrecht ausgeführt wird und damit das EGovG (des Bundes) nicht gilt. Diese Lücke ist zu schließen. In diesem Zusammenhang ist, wie in § 6 EGovG, auch eine Regelung zur Einführung der elektronischen Akte notwendig. Sie ist nicht nur eine wesentliche Grundvoraussetzung für Open Government und Open Data und eine medienbruchfreie Kommunikation, sondern auch erforderlich für die zur Verfügungstellung offener maschinenlesbarer Daten im Sinne der Public-Sector-Information-Richtlinie (PSI-RL), zu deren Umsetzung die Mitgliedsstaaten der EU bis zum 18. Juli 2015 verpflichtet sind. Eine Anpassung der IT-Strategie „Sachsen-Anhalt digital 2020“ wäre auch mit Blick auf die Digitale Agenda 2020 des Bundes geboten. Eine Ergänzung durch eine Open Government- und Open Data-Strategie ist notwendig.

   Der Entwurf eines Organisationsgesetzes Sachsen-Anhalt (OrgG LSA) vom 3. Juni 2014 (LT-Drs. 6/3155) trifft für die *Elektronische Verwaltung* (§ 3) grundsätzliche Regelungen. Das Nähere ist nach § 3 Abs. 3 des Entwurfs durch ein weiteres *Gesetz*, das diese Prinzipien umsetzen soll, zu regeln. Denkbar wäre es z. B., wie bereits in Sachsen mit dem *SächsEGovG* erfolgt, Näheres dieser *Elektronischen Verw*altung in einem E- und Open-Government-Gesetz Sachsen-Anhalt zu regeln.

4. Landesinformationsregister

Ich habe mehrfach das hohe Wirtschaftspotential von Open Data betont und in diesem Zusammenhang darauf hingewiesen, dass Sachsen-Anhalt dieses Potential derzeit nicht nutzt, da die Landesregierung bisher von dem Aufbau eines landesweiten Informationsregisters / Open-Data-Portal abgesehen und auch keine ausdrücklich gesetzliche Regelung für ein landeseigenes Open-Data-Portal bzw. ein Informationsregister im Informationszugangsgesetz Sachsen-Anhalt (IZG LSA) geschaffen hat.
Die Landesregierung hat in ihrer Kabinettssitzung am 15. April 2014 zumindest den Masterplan Landesportal 2014 - 2016 beschlossen, demzufolge das Landesportal zu einem Informationsregister weiterentwickelt werden soll. Der Masterplan sieht daher ab dem Jahr 2015 den Aufbau eines Informationsregisters vor, in dem amtliche Informationen nach Maßgabe des IZG LSA bzw. des bereichsspezifischen Informationszugangsrechts veröffentlicht werden.

5. Landesleitlinie Informationssicherheit zügig verabschieden!

Die Landesleitlinie Informationssicherheit, die eine der Voraussetzungen zum Anschluss des Landes an das Verbindungsnetz gemäß § 3 des IT-NetzG ab dem 1. Januar 2015 bildet, ist bisher noch nicht verabschiedet. Sie sieht zwar den *Datenschutz* als festen Bestandteil des IT-Sicherheitsmanagement vor, hat aber nur empfehlenden Charakter für den kommunalen Bereich. Eine durchgängige Sicherheit bei Ebenen-übergreifenden Verfahren ist so nicht gewährleistet.

6. Rahmenvereinbarung Land – Kommunen

Die Rahmenvereinbarung über die Zusammenarbeit in den Bereichen Informations- und Kommunikationstechnologie sowie E-Government zwischen der Landesregierung und den kommunalen Spitzenverbänden vom 16. Juli 2014 beinhaltet lediglich Ziele und Grundsätze. Aus dem festgelegten Rahmen lassen allerdings keine konkrete Maßnahmen ableiten.

7. Neues Landesnetz – ITN-XT

Mit dem Kabinettbeschluss vom 8. Mai 2012 wurde der CIO des Landes beauftragt, die Leistungsbeschreibung für das neue Landessprach- und Datennetz (ITN-XT) zu erarbeiten. Das Projekt ITN-XT ist eines der Projekte im *Umsetzungsplan* der Strategie Sachsen-Anhalt digital 2020. Die Anforderungen des Datenschutzes und der Datensicherheit sollte bei der Ausschreibung und dem Vergabeverfahren Berücksichtigung finden. Der

Landesbeauftragte für den Datenschutz sollte hier beteiligt werden, das ist bisher unter datenschutzrechtlichem Gesichtspunkt unterblieben. Der Betrieb des neuen Netzes dürfte kaum zum geplanten Starttermin Anfang 2015 gelingen.

8. Exkurs: Einführung des Elektronischen Rechtsverkehrs in der Justiz

Nach dem Gesetz zur Förderung des elektronischen Rechtsverkehrs soll ab dem 1. Januar 2018 der elektronische Zugang zu allen Gerichten grundsätzlich eröffnet werden (vgl. EGVP – Einheitliches Gerichts- und Verwaltungspostfach). Den Ländern wurde die Möglichkeit eingeräumt, die elektronische Erreichbarkeit ihrer Gerichte bis zum 1. Januar 2020 zu verschieben. Hierzu hat das Ministerium der Justiz ein Strategiegremium, einen Lenkungskreis sowie entsprechende Arbeitsgruppen eingerichtet. Die Landesregierung plant für 2015 die Pilotierung des Projektes elektronische Akte wohl aber nur im Geschäftsbereich der Justiz, obwohl in allen Bereichen der Landesverwaltung diese Einführung erforderlich wäre. Die spezifischen Anforderungen an die elektronische Akte im Justizbereich lassen sich nicht ohne weiteres auf die übrigen Behörden der Landesverwaltung übertragen. Eventuelle Auswirkungen der Verordnung des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 16. Juli 2014 (2012/0146 (COD)) sind zu prüfen.

Fazit:

Wie bereits im XI. Tätigkeitsbericht (Nr. 4.2, S. 36) sowie in der Stellungnahme zur Anhörung am 19. April 2013 vor der Enquete-Kommission empfehle ich eine ganzheitliche, nachhaltige, verbindliche, vernetzte und die Datensicherheit einbeziehende Strategie. Es sollte ein Ruck durch das Land gehen. Ungeachtet klarer Strategien und Konzepte sollte auch das Handeln nicht vergessen werden. Der Landesbeauftragte versteht sich bei aller unvermeidlichen Kritik als unabhängiger Ansprechpartner und Berater bei der Gestaltung und Umsetzung eines zukunftsfähigen E-Governments, damit die grundrechtlichen Dimensionen des informationellen Selbstbestimmungsrechts und die Integrität und Vertraulichkeit informationstechnischer Systeme beachtet und gewährleistet werden.

<u>Anhang I</u>:

Maßnahmen des Bundes – Digitale Agenda 2014 – 2017 der Bundesregierung

Ausgewählte Grundsätze und Maßnahmen zu Datenschutz und Informationsfreiheit der am 20. August 2014 von der Bundesregierung vorgestellten „Digitalen Agenda 2014 – 2017“ sind:

III. Innovativer Staat

- Der Bund beabsichtigt eng mit Ländern und Kommunen zusammen zu arbeiten und die Entwicklung nutzerfreundlicher *kommunaler* E-Government Angebote zu fördern.

- Bürgerinnen und Bürger sollen mit der Verwaltung einfach und sicher kommunizieren können. Es werden deshalb gemeinsam mit den Ländern Bürgerkonten eingerichtet, bei denen die sichere Authentifizierung auch mit der *eID-Funktion des Personalausweises* erfolgt und mit denen möglichst viele Verwaltungsdienstleistungen auf kommunaler, Länder-und Bundesebene einfach und sicher genutzt werden können.

- Elektronische Dienste der Verwaltung erfordern effiziente Schnittstellen zwischen Verwaltung und Bürgerinnen und Bürgern sowie Unternehmen. Es sollen bestehende, Ebenen übergreifende Lösungen – wie bereits bei der einheitlichen Behördenrufnummer 115 oder dem *einheitlichen Ansprechpartner* – weiter ausgebaut werden. Alle nutzenbringenden Dienstleistungen der Verwaltung sollen online zur Verfügung gestellt werden.

- *Flächendeckende* Einführung von *De-Mail*. Um die flächendeckende Einführung von De-Mail zu beschleunigen, wird eine gemeinsame Arbeitsgruppe mit der Wirtschaft eingerichtet, in der Erfahrungen ausgetauscht und identifizierte Hürden zeitnah adressiert werden.

- Prüfung und ersatzlose *Streichung verwaltungsrechtlicher Formerfordernisse*, soweit möglich.

- Bundesbehörden sollen Vorreiter bei der Bereitstellung offener Daten werden (*Open Data*).

VI. Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft

- Vereinfachung der Nutzung des neuen Personalausweises
- **„Deutschland soll Verschlüsselungsstandort Nr. 1 in der Welt werden."**
- **IT-Sicherheitsgesetz** (Kritik: Vorratsdatenspeicherung durch die Hintertür!)
- Die Datenschutz-Grundverordnung soll spätestens 2015 verabschiedet werden
- Die Bundesregierung strebt eine führende Rolle bei der Entwicklung internationaler Datenschutzprinzipien an.

<u>Anhang II</u>:

Übersicht wesentlicher Rechtsmaterien

1. Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (**EU-Signaturrichtlinie**) (ABl. L 13 vom 19.01.2000 S. 12)

2. Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („**Richtlinie über den elektronischen Geschäftsverkehr**"; auch „**E-Commerce-Richtlinie**" genannt) ABl. L 178 vom 17.07.2000 S. 1)

3. Die ***elektronische Form*** ist in **§ 126a** des Bürgerlichen Gesetzbuches (BGB) definiert. Das Formanpassungsgesetz vom: 13. Juli 2001 (BGBl. I S. 1542), Inkrafttreten am: 1. August 2001, dient zur Regelung der materiell-rechtlichen Gleichstellung der elektronischen Signatur an die Handunterschrift im modernen Rechtsgeschäftsverkehr. Die elektronische Form entspricht grundsätzlich der Schriftform.

   § 126a BGB lautet: „Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer **qualifizierten elektronischen Signatur** nach dem Signaturgesetz versehen." Mit der Bestimmung setzte der Gesetzgeber Art. 9 der E-Commerce-Richtlinie sowie Art. 5 der EU-Signaturrichtlinie um (materiell rechtliche Anerkennung).

4. Gesetz über Rahmenbedingungen für elektronische Signaturen (**Signaturgesetz** - SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

5. Verordnung zur elektronischen Signatur (**Signaturverordnung** - SigV) Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

6. Verwaltungsverfahrensgesetz (VwVfG**)** in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), zuletzt geändert durch Artikel 3 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749)

7. Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt (**EU-Dienstleistungsrichtlinie** - EU-DLR; (ABl. EU Nr. L 376 S. 36)

8. Gesetz über Personalausweise und den **elektronischen Identitätsnachweis** (**Personalausweisgesetz** - PAuswG) vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Artikel 2 Absatz 13 u. Artikel 4 Absatz 1 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

9. **Verbindungsnetz** (IT-NetzG) „Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG)“ vom 10. August 2009.

10. **De-Mail-Gesetz** (De-MailG) vom 28. April 2011 (BGBl. I S. 666), zuletzt geändert durch Artikel 3 Absatz 8 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

11. Gesetz zur Förderung der elektronischen Verwaltung (**E-Government-Gesetz** - EGovG) vom 25. Juli 2013 (BGBl. I S. 2749)

12. **Verordnung** des Europäischen Parlaments und des Rates
über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 16. Juli 2014 (2012/0146 (COD))

(VwVfG)

§ 3a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem

Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4. durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

(Sächsisches E-Government-Gesetz - SächsEGovG vom 9. Juli 2014**)**

§ 2 Elektronische Kommunikation

(1) 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. (...)