Bundesministerium
für Wirtschaft
und Arbeit

Rechtskonformes E-Government

Antworten auf Kernfragen beim Bau eines virtuellen Rathauses

erfolgsmodell
kommunales
e-government

MEDIA@Komm

Rechtskonformes E-Government

Antworten auf Kernfragen beim Bau eines virtuellen Rathauses

Martin Eifert
Jan Ole Püschel
Claudia Stapel-Schulz

Dieser Leitfaden ist mit großer Sorgfalt erstellt worden. Dennoch können weder die Verfasser noch der Herausgeber eine Verantwortung bzw. Haftung für die Richtigkeit, Vollständigkeit oder Aktualität der Angaben im Leitfaden übernehmen. Nur um eine verbesserte Lesbarkeit des Textes zu erreichen, wird teilweise lediglich das männliche grammatikalische Geschlecht verwendet.

Die Broschüre entstand im Rahmen
der Begleitforschung zum Leitprojekt *MEDIA*@Komm

MEDIA@Komm ist ein Förderprojekt
des Bundesministeriums für Wirtschaft und Arbeit

Bundesministerium
für Wirtschaft
und Arbeit

Vorwort

von Wolfgang Clement
Bundesminister für Wirtschaft und Arbeit
für den Leitfaden Rechtskonformes E-Government

E-Government ist eines der Instrumente, mit denen wir unserem Ziel, bürokratische Hürden abzubauen, die Leistungsfähigkeit unserer Unternehmen zu stärken und ihre Position im Standortwettbewerb zu verbessern, hoffentlich schnell näherkommen. Die Unternehmen profitieren von E-Government in vielerlei Hinsicht, als Produzenten, Zulieferer und Betreiber. Bürgerinnen und Bürger, die Online-Vernetzung mit öffentlichen Verwaltungen nutzen, können zunehmend auf Behördengänge verzichten; sie erhalten schnellstmögliche Informationen und können neue Möglichkeiten der gesellschaftliche Teilhabe nutzen.

Die mit Abstand meisten Verwaltungskontakte erfolgen auf kommunaler Ebene. Dem „virtuellen Rathaus" kommt folglich eine zentrale Bedeutung zu. Hiervon können auch die kleinen und mittleren Unternehmen profitieren. Sie sind auf präzise und rasch und leicht zugängliche Informationen und ganz besonders auf ein unbürokratisches und effizientes Verhältnis zu den öffentlichen Verwaltungen angewiesen.

Mit dem Start des *MEDIA*@Komm-Projekts vor drei Jahren hat das Bundesministerium für Wirtschaft und Arbeit hier einen Schwerpunkt gesetzt. Im Rahmen dieses Vorhabens werden bis Ende des Jahres in den Modellregionen Bremen, Esslingen und Nürnberg virtuelle Rathäuser und virtuelle Marktplätze geschaffen und auch erprobt. Im Mittelpunkt der Arbeiten steht dabei der nahtlose Übergang von Information und Kommunikation in digitalen Netzen zu elektronischen Transaktions- und Partizipationsprozessen.

MEDIA@Komm ist das Leitprojekt der Bundesregierung für kommunales E-Government. Es ergänzt die Initiative BundOnline2005, mit der bis 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung im digitalen Netz verfügbar sein werden. Die *MEDIA*@Komm-Aktivitäten, die vom elektronischen Meldewesen über das virtuelle Bauamt bis hin zur netzbasierten Bürgerbeteiligung bei Planungsprozessen reichen, finden zunehmend Nachahmer; Folgeinvestitionen schließen sich an, was sich auch auf die weitere Einführung der gesetzeskonformen elektronischen Signatur auswirkt.

Dies alles verdeutlicht aber auch, dass Electronic Government nur dann wirklich Tritt fassen kann, wenn die noch nötigen technischen Lösungen bald gefunden sind, die Verwaltung entschlossen und ohne Berührungsängste mitwirkt und auch über den zugrunde liegenden Rechtsrahmen informiert ist. Hierbei wird dieser Ratgeber helfen. Er will kommunalen Entscheidungsträgern und Rechtsexperten eine Orientierung über die juristischen Fragen geben, die bei kommunalen Electronic-Government-Projekten zu beachten sind, ohne die rechtliche Prüfung im Einzelfall zu ersetzen.

Ich hoffe, dass der Leitfaden die Verbreitung von E-Government auf kommunaler Ebene fördert und dadurch die dringend notwendige Modernisierung unseres Gemeinwesens mit positiven Impulsen für den Wirtschaftsstandort Deutschland voranbringt.

Wolfgang Clement
Bundesminister für
Wirtschaft und Arbeit

Danksagung

Der vorliegende Leitfaden beruht auch auf der Erfahrung, die wir im Rahmen der rechtswissenschaftlichen Begleitung *MEDIA*@Komm-Preisträgerstädte Bremen, Esslingen und Städteverbund Nürnberg gewinnen konnten. Wir möchten deshalb insbesondere den fachlichen Diskussionspartnern in diesen Städten herzlich für die produktive Zusammenarbeit danken, insbesondere Herrn Dr. Andreas Bovenschulte (Bremen-Online-Services), Herrn Klaus Eisele (Stadt Nürnberg) sowie Herrn Karsten Rössler (*MEDIA*@Komm Esslingen).

Die datenschutzrechtlichen Teile des Leitfadens wurden meist nicht von den Autoren verfasst, sondern greifen ausweislich der Zitierung auf die Bewertungen der Datenschutzbeauftragten von Bund und Ländern zurück. Sie sind dem umfassenden Ratgeber „Datenschutzgerechtes eGovernment" entnommen, den die Datenschutzbeauftragten von Bund und Ländern erstellt haben und der für die datenschutzrechtlichen Fragen unbedingt herangezogen werden sollte. Wir danken stellvertretend dem federführenden Landesdatenschutzbeauftragten für das Land Niedersachsen, Herrn Burckhard Nedden, ganz herzlich für die Genehmigung zum teilweisen Abdruck. Herr Prof. Dr. Alexander Roßnagel, der auch dem Beirat von *MEDIA*@Komm angehört, war so freundlich, den Entwurf des Leitfadens kritisch durchzusehen. Wir danken ihm sehr herzlich für diese Mühe und seine wertvollen Anmerkungen.

Schließlich möchten wir uns ebenfalls sehr herzlich bei Herrn Dr. Lutz Schreiber bedanken, der knapp zwei Jahre in der rechtswissenschaftlichen Begleitforschung mitarbeitete und erheblichen Anteil an ihrem Gelingen hatte. Das gleiche gilt für die studentischen Hilfskräfte Arne Fahje, Sebastian Janka, Maja Kreßin, Jens Neubert, Beatrice Stange, Lilian Unger und vor allem Christian Braune und Katharina Jenssen, die uns in verschiedenen Zeiten des Projekts tatkräftig unterstützten.

Hamburg im Januar 2003 — Martin Eifert, Jan Ole Püschel, Claudia Stapel-Schulz

Inhaltsverzeichnis

Vorwort 5

Danksagung 6

Inhaltsverzeichnis 7

Abbildungsverzeichnis 10

Hinweise zu Aufbau und Nutzung des Leitfadens 11

1. Die Sicherung der städtischen Domain 12

1.1 Hat die Stadt einen Anspruch auf die Domain „www.stadtname.de“? 12

1.2 Können sich auch einzelne Behörden oder Teile einer Behörde auf ein Namensrecht berufen? 12

1.3 Besteht auch ein Anspruch auf eine Domain, die den Stadtnamen nur als Teil enthält? 12

1.4 Was kann bei einer Verletzung des Namensrechts unternommen werden? 13

1.5 Was ist bei anderen Top-Level-Domains zu beachten? 13

2. Portalangebote der Stadt 14

2.1 Welche Angebote auf dem Portal sind kommunalwirtschaftsrechtlich zulässig? 14
2.1.1 Was sind die zu beachtenden Vorgaben? 14
2.1.2 Welche Informationsangebote sind zulässig? 15
2.1.3 Welche Kommunikationsangebote sind zulässig? 18
2.1.4 Welche Transaktionsangebote sind zulässig? 18
2.1.5 Sind Mehrwertdienste zulässig? 18
2.1.6 Ist Werbung auf den Portalseiten zulässig? 19
2.1.7 Unter welchen Voraussetzungen können überregionale private Angebote integriert werden? 19

2.2 Kann die Verwaltung selbst Aufgaben nach SigG/ SigV wahrnehmen? 20

3. Organisationsformen für städtische Portale 21

3.1 Welche allgemeinen Grundsätze sind bei der Auswahl einer Organisationsform zu beachten? 23

3.2 Was ist bei einer öffentlich-rechtlichen Organisationsform zu bedenken? 24

3.3 Was ist bei einer privatrechtlichen Organisationsform mit städtischer Beteiligung zu bedenken? 24
3.3.1 Was ist bei der Gründung eines gemischt wirtschaftlichen Unternehmens zu beden ken? 24
3.3.2 Was ist bei einer Gründung eines Vereins grundsätzlich zu bedenken? 32

3.4 Was ist bei einem vollständig privaten Betrieb zu bedenken? 32
3.4.1 Was ist bei der Auswahl der privaten Partner zu beachten? 32
3.4.2 Was ist im Betreibervertrag zu regeln ? 33
3.4.3 Sind Exklusivvereinbarungen zulässig? 33

3.5 Interkommunale Zusammenarbeit 34

3.6 Was ist aus datenschutzrechtlicher Sicht bei einer Aufgabenübertragung an Dritte zu beachten? 35

4. Einbindung privaten IT- Know Hows 37

4.1 Was ist bei Einzelverträge über IT-Leistungen/Outsourcing zu bedenken? 37
4.1.1 Was ist bei der Auswahl der privaten Partner zu beachten? 37
4.1.2 Welche Regelungsaspekte sollten umfasst werden? 39

4.2 Was ist beim Eingehen von Entwicklungspartnerschaften zu bedenken? 40
4.2.1 Was ist bei der Auswahl der privaten Partner zu beachten? 40
4.2.2 Welche Regelungsaspekte sollten umfasst werden? 41

5. Allgemeine Vorgaben für alle Angebotstypen 42

5.1 Wie sind die einzelnen Angebote medienrechtlich einzuordnen? 42

5.2 Bestehen abweichende Anforderungen an Medien- und Teledienste? 42

5.3 Welche allgemeinen Haftungsgrundsätze sind zu beachten? 43

5.4 Welche allgemeinen Kennzeichenpflichten sind zu beachten? 43

5.5 Wie sind Datenschutzhinweise durch die Verwaltung auszugestalten? 44

5.6 Was ist für die Einbeziehung von Benutzungsbedingungen, Haftungsausschlüssen und Datenschutzhinweisen zu beachten? 45

5.7 Welche allgemeinen Datenschutzgrundsätze sind bei einer Internettätigkeit der Verwaltung zu beachten? 45
5.7.1 Welche gesetzlichen Grundlagen sind für ein datenschutzgerechtes E-Government relevant? 45
5.7.2 Welche grundsätzlichen Anforderungen bestehen für die Erhebung und Verarbeitung von personenbezogenen Daten? 47
5.7.3 Wie kann eine datenschutzrechtliche Einwilligung online erfolgen? 47
5.7.4 Was folgt aus dem Grundsatz der Datenvermeidung und Datensparsamkeit? 48
5.7.5 Was folgt aus dem Grundsatz der Zweckbindung? 48
5.7.6 Was folgt aus dem Grundsatz der Erforderlichkeit? 48
5.7.7 Was folgt für die Verwaltung aus dem Grundsatz der informationellen Gewaltenteilung 49
5.7.8 Welcher Anspruch besteht für den Betroffenen hinsichtlich Berichtigung, Löschung oder Sperrung personenbezogener Daten? 50
5.7.9 Welche datenschutzrechtlichen Vorgaben bestehen für eine virtuelle Poststelle der Verwaltung? 50
5.7.10 Was ist aus datenschutzrechtlicher Sicht bei der Speicherung von Grunddaten des Bürgers zu beachten? 50

5.8 Welche rechtlichen Vorgaben sind hinsichtlich der Gleichstellung von Behinderten zu berücksichtigen? 51
5.8.1 Was folgt aus dem Gesetz zur Gleichstellung behinderter Menschen? 51
5.8.2 Was folgt aus der Barrierefreie Informationstechnik-Verordnung? 52
5.8.3 Enthält auch das SGB IX Vorgaben für die Verwaltung? 52

5.9 Welche Anbieterpflichten folgen für das Angebot der Verwaltung aus der Qualifizierung als öffentliche Einrichtung? 52
5.9.1 Wann sind das Portal oder einzelne Portalangebote als öffentliche Einrichtung zu qualifizieren? 52
5.9.2 Welche Ansprüche haben die Einwohner bei einer Einordnung als öffentliche Einrichtung? 53

5.10 Was ist grundsätzlich bei Dienstanweisungen oder Betriebsvereinbarungen für den Einsatz von Informtationstechnik am Arbeitsplatz zu beachten? 53
5.10.1 Für welche Bereiche ist eine Regelung durch Dienstanweisungen oder Betriebsvereinbarungen sinnvoll? 53

5.10.2 In wieweit ist neben der Personalvertretung auch der behördliche Datenschutzbeauftragte zu beteiligen? 54
5.10.3 Welche Regelungsaspekte sollten von Dienstanweisungen bzw. Betriebsvereinbarungen umfasst werden? 55

6. Spezifische Vorgaben für die einzelnen Angebotstypen 56

6.1 Was ist bei Informationsangeboten zu beachten? 56
6.1.1. Welche datenschutzrechtlichen Vorgaben sind für Informationsdienste der Verwaltung zu beachten? 56
6.1.2. Wer haftet für Informationsinhalte? 57
6.1.3. Was ist bei der Integration fremder Informationsinhalte zu bedenken? 58

6.2 Was ist bei Kommunikationsangeboten zu beachten? 59
6.2.1 Was ist bei Kommunikation via E-Mail zu beachten? 59
6.2.2 Was ist bei der Veranstaltung von öffentlichen Diskussionsforen durch die Verwaltung zu beachten? 63

6.3 Was ist für Transaktionsangebote zu berücksichtigen? 65
6.3.1 Unter welchen Voraussetzungen kann zwischen Bürger und Verwaltung eine rechtsverbindliche Online-Transaktion stattfinden? 66
6.3.2 Wie funktioniert die qualifizierte elektronische Signatur? 66
6.3.3 Welche Signaturen für die Verwaltung? – Die unterschiedlichen Regelungsniveaus 67
6.3.4 Welche Regelungsaspekte gelten für Rahmenverträge zwischen Verwaltung und privaten Zertifizierungsdiensteanbietern? 71
6.3.5 Welche Vorgaben bestehen für den Inhalt von Zertifikaten? 72
6.3.6 Ist auch die Verwendung von Software-Signaturen zulässig? 73
6.3.7. Welche Beweiskraft haben Dokumente mit elektronischer Signatur? 74
6.3.8. Bestehen beim unbefugten Einsatz der Signaturkarte mit PIN durch einen Dritten Haftungsrisiken für die Verwaltungsbediensteten? 75
6.3.9. Müssen Anlagen zu einem signierten Antrag ebenfalls signiert werden? 75
6.3.10. Wie können elektronische Dokumente durch die Behörde beglaubigt werden? 75

6.4. Was ist durch die Verwaltung bei elektronischen Verwaltungsakten zu beachten? 76
6.4.1. Sind elektronische Verwaltungsakte nur mit elektronischer Signatur zulässig? 76
6.4.2. Ist eine gesonderte elektronische Rechtsbehelfsbelehrung formgebunden? 76
6.4.3. Welche Anforderungen bestehen hinsichtlich des Zugangs von elektronischen Erklärungen oder Verwaltungsakten? 77
6.4.4. Wie kann eine Beweissicherung des Zugangs erfolgen? 78
6.4.5. Welche Anforderungen bestehen an die elek-tronische Begründung eines Verwaltungsaktes? 78
6.4.6. Dürfen Verwaltungsakte auch elektronisch bestätigt werden? 79
6.4.7. Welche Anforderungen bestehen an eine elektronische Aktenführung? 79
6.4.8. Was ist aus datenschutzrechtlicher Sicht für eine elektronische Aktenführung beachtlich? 79

6.5. Welche rechtlichen Probleme können bzgl. des Zugangs zu Online-Transaktionsangeboten der Verwaltung auftreten? 84
6.5.1. Muss die Verwaltung alle Signaturen akzeptieren? 84
6.5.2. Welche technischen Vorgaben darf die Verwaltung für Signaturen treffen? 84
6.5.3. Darf die Verwaltung vom Bürger ein höheres Signaturniveau als gesetzlich gefordert verlangen ? 84
6.5.4. Darf die Verwaltung ein höheres Signaturniveau verwenden? 84
6.5.5. Muss die Verwaltung auch elektronische Signaturen ausländischer Zertifizierungsdiensteanbieter akzeptieren? 84
6.5.6. Welche rechtlichen Konsequenzen ergeben sich durch eine fehlgeschlagene Signaturprüfung? 85
6.5.7. Ist der Aussteller eines elektronischen Dokuments eindeutig zu identifizieren? 85

6.6. Was ist bei der Elektronischen Vergabe zu beachten? 86

6.7. Welche Modelle kommen für ein rechtskonformes Key-Management in Betracht? 87
6.7.1. Die Verwendung von personenbezogenen Hauptzertifikaten mit Namen des Schlüsselinhabers 88
6.7.2. Das Modell der Verwendung von Attributzertifikaten 88

6.7.3. Das Modell der pseudonymisierten aufgabenbezogenen Zertifikate 88
6.7.4. Das Modell verwaltungseigener Signaturserver (Sicherheitsbox) 89

6.8. Welche Anforderungen sind aus rechtlicher Sicht an die durch die Behörde eingesetzten Signaturkomponenten zu stellen? 89
6.8.1. Welche Anforderungen bestehen für Signaturkomponenten qualifizierter Signaturen ? 89
6.8.2. Welche Anforderungen bestehen für Signaturkomponenten von akkreditierten Signaturen? 90
6.8.3. Muss das gesamte zu signierende Dokument am Bildschirm für den Signierenden sichtbar gemacht werden? 90

6.9. Welche rechtlichen Probleme können durch das Angebot des E-Payments für die Verwaltung entstehen? 90
6.9.1. Welche rechtlichen Anforderungen bestehen für die Nutzung der Kreditkarte als Online-Zahlungsmittel für Dienstleistungen der Verwaltung? 90
6.9.2. Besteht die rechtliche Notwendigkeit anonymer Bezahlverfahren für Angebote der Verwaltung? 91

6.10. Dürfen die Gebühren für Online-Verwaltungsdienste von den allgemeinen Gebührensätzen abweichen? 91

Abkürzungsverzeichnis **93**

Stichwortverzeichnis **96**

Zu den Autoren **99**

Abbildungsverzeichnis

Abbildung 1	Zulässigkeit von Informationsangeboten	Seite 16
Abbildung 2	Wahl einer Organisationsform	Seite 22
Abbildung 3	Das Vergabeverfahren – Übersicht –	Seite 28
Abbildung 4	Regelungsebenen im Datenschutz	Seite 46
Abbildung 5	Signaturen und ihre rechtlichen Unterschiede im Überblick	Seite 69, 70, 71
Abbildung 6	Elektronisches (Leistungs-) Verwaltungsverfahren	Seite 83

Hinweise zu Aufbau und Nutzung des Leitfadens

Der Leitfaden behandelt die rechtlichen Fragen des Electronic Government entlang des typischen Entwicklungspfades der kommunalen Rathäuser und an Hand der sich dabei regelmäßig stellenden Fragen. Er bietet damit sowohl eine kontinuierliche Begleitung während des Aufbaus eines virtuellen Rathauses als auch eine punktuelle Orientierung bei einzelnen Ausbaustufen oder Fragenkomplexen.

Der Entwicklungspfad beginnt bei der Sicherung einer Domain. Er setzt sich über die strategisch bedeutsame Frage der zulässigen kommunalen Angebote und die u.a. angebotsabhängigen Organisationsmodelle fort bis zu den Rechtsfragen der Ausgestaltung der einzelnen Angebotstypen. Dabei wird nach der Darstellung übergreifender Anforderungen wiederum entsprechend der typischen Entwicklung unterschieden und zunächst auf die Informationsangebote und dann auf die Kommunikations- und Transaktionsangebote näher eingegangen.

Die rechtssystematisch aus verschiedenen Gebieten stammenden Anforderungen (z.B. Datenschutzrecht, Kommunalrecht, Vergaberecht, Verwaltungsverfahrensrecht, Recht der elektronischen Signaturen) wurden jeweils unter den praxisorientierten Fragestellungen gebündelt. Die Darstellung ist damit vor allem auf einen Zugriff entsprechend der Sachprobleme ausgerichtet. Das Stichwortverzeichnis ermöglicht allerdings auch einen hiervon abweichenden Zugriff auf einzelne Rechtsfragen.

Der Leitfaden zielt auf eine Darstellung des Rechtsrahmens ab und will eine Orientierungsmöglichkeit hinsichtlich der auftretenden Rechtsfragen insbesondere für kommunale Entscheider sein. Im Hinblick auf die Anforderungen an die konkreten Angebote der Verwaltung gilt dieser Rechtsrahmen jedoch für alle Verwaltungsebenen. Die Orientierungsfunktion erfordert eine Praxisorientierung, ein Mindestmaß an Übersichtlichkeit und eine Beschränkung des Umfangs. Der Leitfaden ist deshalb vor allem bei divergierenden Rechtslagen in den verschiedenen Ländern und in Bereichen hochdifferenzierter rechtlicher Anforderungen allgemeiner gehalten. Er vertieft auch keine rechtlichen Streitfragen und folgt soweit möglich der bestehenden Rechtsprechungspraxis. Er kann und soll deshalb insgesamt eine detaillierte, einzelfallbezogene Rechtsprüfung und -beratung nicht ersetzen.

Für eine Vertiefung der datenschutzrechtlichen Fragen möchten wir auf den Leitfaden „Datenschutzgerechtes eGovernment" der Datenschutzbeauftragten von Bund und Ländern verweisen, dem auch die datenschutzrechtlichen Teile dieses Leitfadens im wesentlichen entnommen wurden. Er kann unter www.lfd.niedersachsen.de oder www.datenschutz.de abgerufen werden.

1. Die Sicherung der städtischen Domain

Für eine Präsenz im Internet muss die Kommune oder Stadt eine Internetadresse (Domain) bei der zuständigen Stelle registrieren lassen, i.d.R. die naheliegende Domain „www.stadtname.de“. Um auch diejenigen Nutzer zu erreichen, die den Namen der Stadt falsch eintippen, ist auch eine Registrierung des Stadtnamens mit abweichenden Schreibweisen sinnvoll. Für die Vergabe von Adressen mit dem Kürzel „.de“ ist die nichtamtliche deutsche Vergabestelle DENIC e.G. zuständig (www.denic.de). Die Vergabe richtet sich nach dem Prioritätsprinzip, d.h. „first come, first serve“, unabhängig von möglichen betroffenen Rechten Dritter. Eine Registrierung nach dem Prioritätsprinzip entfaltet allerdings keine abschließend geschützte Rechtsposition für den Erst-Registrierer. Kann ein Dritter nachträglich ein besseres Recht geltend machen, muss der Erst-Registrierer die Domain wieder freigeben. Ist die begehrte Domain www.stadtname.de bereits vergeben, kann über die DENIC e.G. in Erfahrung gebracht werden, wer sich für die Domain registriert hat.

1.1 Hat die Stadt einen Anspruch auf die Domain „www.stadtname.de“?

Für die Frage, ob der Stadt ein Recht an der Domain „www.stadtname.de“ zusteht, gibt es mittlerweile eine umfassende Rechtsprechung bei der sich inzwischen auch eine gefestigte Linie abzeichnet. Die zentrale Anspruchsnorm ergibt sich aus dem Namensrecht des § 12 BGB, da Städtenamen nach dieser Vorschrift auch ohne den Zusatz „Stadt“ namensrechtlich geschützt sind. Dies gilt grundsätzlich auch für Gemeindekurzbezeichnungen. Im Hinblick auf den Anspruch der Stadt sind **drei Fallgruppen zu unterscheiden**:

- Bei einem sog. **„Domaingrabbing“** beabsichtigt der Erst-Registrierer nicht die eigene Nutzung der Domain, sondern die Verhinderung der Nutzung durch die Stadt, um von der Stadt einen möglichst hohen Preis für die Ummeldung zu verlangen. Hier liegt in Form der Namensbestreitung unzweifelhaft eine Namensrechtsverletzung nach § 12 Bürgerliches Gesetzbuch (BGB) vor.
- Hat der Erst-Registrierer die Domain frei gewählt, ohne selbst Namensträger zu sein, liegt eine Verletzung des Namensrechts nach § 12 BGB in Form der **Namensanmaßung** vor. Da der Namensschutz insbesondere einer Zuordnungsverwirrung entgegenwirken soll, wird die Verletzung eines schutzwürdigen Interesses des Namensberechtigten von der Rechtsprechung damit begründet, dass der Nutzer die Domain mit der Stadt verbinde bzw. hinter der Domain die offizielle Präsentation der Stadt erwarte und der Private selbst kein schutzwürdiges namensrechtliches Interesse habe.
- Ist der Erst-Registrierer selbst ebenfalls Träger des bürgerlichen Namens, löst die Rechtsprechung diesen Konflikt mittels einer **Interessenabwägung** zwischen den berechtigten Namensträgern. Hier gilt allgemein der Grundsatz der Priorität. Von ihm kann ausnahmsweise zugunsten der Stadt in folgenden Fällen abgewichen werden: bei Domaingrabbing, aus Gründen des Allgemeinwohls oder bei einer überragenden Bekanntheit der Gebietskörperschaft. Das Vorliegen dieser Gesichtspunkte wurde von der Rechtsprechung bei Streitigkeiten zu den Domains „boos.de“, „tschirn.de“ oder „vallendar.de“ aber nicht angenommen.

Abschließend kann festgehalten werden, dass die Stadt oder Kommune ein Recht auf die städtische Domain „www.stadtname.de“ gegenüber jedermann hat, dem kein vorrangiges Namensrecht auf diesen Namen zusteht.

1.2 Können sich auch einzelne Behörden oder Teile einer Behörde auf ein Namensrecht berufen?

Auf den Namensschutz können sich auch juristische Personen des öffentlichen Rechts hinsichtlich solcher Bezeichnungen mit Erfolg berufen, denen **Kennzeichnungscharakter** und **Bezug zur politischen Körperschaft** zukommen. So wird z.B. Behörden oder zusammengesetzten Namen wie „polizeibrandenburg.de“ ein Schutz zuerkannt, wenn der Domainname den Eindruck erweckt, dass sich dahinter die entsprechende Gebietskörperschaft verbirgt. Denn bei einer Nutzung durch Private könnte es hier zu einer Zuordnungsverwirrung kommen. Die oben aufgeführten Fallgruppen sind auf diesen Fall übertragbar.

1.3 Besteht auch ein Anspruch auf eine Domain, die den Stadtnamen nur als Teil enthält?

Zu dieser Frage findet sich noch keine gefestigte Rechtsprechung. Ein kürzlich ergangenes Urteil des OLG Düssel-

dorf, das sich auf „www.duisburg-info.de“ bezog, hat einen Anspruch der Stadt Duisburg abgelehnt. Der Entscheidung liegt die Annahme des Gerichts zugrunde, dass der Verkehr nicht davon ausgehe, dass sämtliche Domains, die einen Städtenamen enthalten, von der Stadt oder mit Zustimmung der Stadt gehalten werden. Dies liege zwar nahe bei Domains, die ausschließlich aus der Bezeichnung „www.stadtname.de“ oder mit dem Zusatz „Gemeinde“ oder „Stadt“ gebildet sind. Bei anderen Zusätzen (z.B. „www.stadtname-info.de“) komme es aber darauf an, wie der **Verkehr die Gesamtbezeichnung verstehe**.

1.4 Was kann bei einer Verletzung des Namensrechts unternommen werden?

Der Anspruch der Kommune oder Stadt zielt bei einer Namensrechtsverletzung nach § 12 BGB auf die Beseitigung des bestehenden Zustandes und beinhaltet daher zum einen die **Freigabe der Domain** gegenüber der DENIC e.G. und zum anderen die **Unterlassung der Nutzung der Domain** durch den Nichtberechtigten zu eigenen Zwecken. Um möglichst einen zeitaufwendigen Rechtsstreit zu vermeiden, sollte in einem ersten Schritt eine begründete **Abmahnung** an den Nichtberechtigten gerichtet werden, in dem unter Angabe einer Frist die Freigabe gegenüber der DENIC e.G. und die Unterlassung der Nutzung verlangt wird. Ist dieser nicht bereit, die Domain freizugeben, bleibt der Gerichtsweg in Form der Leistungsklage mit Unterlassungs- und Beseitigungsantrag.
Sind der Kommune oder Stadt bereits Kosten und Aufwendungen entstanden, kann sie dafür gem. § 823 Abs. 1 i.V.m. § 1004 BGB **Schadensersatz** verlangen, im Falle des „Domaingrabbings“ zusätzlich aus § 826 BGB wegen sittenwidriger Behinderung.
Es bietet sich in bestimmten dringlichen Fällen auch an, das Verfahren im Wege des **einstweiligen Rechtsschutzes** durchzuführen, um den Zustand schnellstmöglich zu beenden. Nach §§ 935 f. Zivilprozessordnung (ZPO) muss dabei die erhöhte Dringlichkeit der Entscheidung dargelegt werden.
Um die Anspruchsdurchsetzung nicht zu gefährden und eine Übertragung der Domain durch den Erst-Registrierer auf einen Dritten zu verhindern, sollte ein sog. **„Dispute-Eintrag“** bei der DENIC e.G. gestellt werden. Für diesen Antrag hält die DENIC e.G. nähere Informationen und ein entsprechendes Online-Formular bereit. Als Anhaltspunkt für ein Recht an dem Domainnamen reicht nach Angaben der DENIC e.G. die Verwendung des entsprechenden Briefkopfes der Gemeinde. Der Dispute-Eintrag endet mit der Beendigung der Auseinandersetzung um die Domain oder spätestens ein Jahr nach Antragstellung.

1.5 Was ist bei anderen Top-Level-Domains zu beachten?

Als verfügbare Top-Level-Domains ohne Landesbezug existieren zum Beispiel die Endungen „**.info**“, „**.net**“, und „**.org**“. Ihre Verwaltung erfolgt über die Internet Corporation for Assigned Names and Numbers (ICANN), die jeweils nationale Registrierungsstellen für die Vergabe der Domains akkreditiert hat. Nähere Informationen sind abzurufen unter www.icann.org. Im Hinblick auf einen namensrechtlichen Anspruch der Stadt auf eine städtische Domain mit den Endungen „.info“, „.net“ und „.org“ vgl. 1.1.
Als Alternative zu einem gerichtlichen Verfahren, z.B. im Hinblick auf die Domain „www.stadtname.net“, besteht bei diesen Domains unter bestimmten festgelegten Voraussetzungen auch die Möglichkeit des sog. **ICANN-Schiedsverfahrens**, das bei allen von der ICANN anerkannten Schlichtungsstellen durchgeführt werden kann (z.B. bei der World Intellectual Property Organisation in Genf: www.wipo.org). Ein Schiedsverfahren geht bei einem internationalen Bezug der Streitigkeit in der Regel wesentlich schneller und ist kostengünstiger als ein gerichtliches Verfahren.

Weiterführende Literatur und Rechtsprechung:
Allgemein zum Domainrecht bei Gebietskörperschaften*: Kröger/Köhn*, Kommunales Namensrecht im Internet, in: Kröger (Hrsg.), Internetstrategien für Kommunen, 2001, S. 395ff.; *Rath-Glawatz*, Die Namen von kommunalen Verwaltungseinheiten im Titel von Medienangeboten, AfP 2002, S. 115ff. Zum Namensrecht von Behörden/Behördenteilen: *LG Hannover*, K&R 2001, S. 652 („verteidigungsministerium.de“). Zum Namensschutz von Gemeindekurzbezeichnungen: *LG Düsseldorf*, Urt v. 16.01.2002, Akz. 2 a O 172/01, JurPC Web-Dok. 398/2002. Zu Domains, die den Stadtnamen nur als Teil enthalten: *OLG Rostock*, K&R 2000, S. 303; *OLG Düsseldorf*, Urt. v. 15.Januar 2002, Akz. 20 U 76/01.

2. Portalangebote der Stadt

2.1 Welche Angebote auf dem Portal sind kommunalwirtschaftsrechtlich zulässig?

Bei der Planung eines städtischen Internetauftritts stellt sich zunächst die Frage, welche Portalangebote die Kommune oder Stadt überhaupt selbst anbieten darf. Dies wird nachfolgend behandelt. Anschließend stellt sich die Frage, welche rechtlichen Vorgaben sie bei der Erfüllung grundsätzlich zulässiger Leistungen beachten muss. Vergleiche dazu 5 und 6.

2.1.1 Was sind die zu beachtenden Vorgaben?

Den zentralen Maßstab für die Zulässigkeit von Internetangeboten auf kommunaler Ebene bilden die sog. **„Wirtschaftsklauseln"** in den Gemeindeordnungen (vgl.: § 107 GO NW, Art. 87 GO Bay, § 102 GO Ba-Wü, § 100 GO Bbg, § 121 HGO, § 68 KV M-V, § 108 NGO, § 85 GO Rh-Pf, § 108 Saarl. KSVG, § 95 SächsGemO, § 116 GO LSA, § 101 GO S-H, § 71 ThürKO). Die Wirtschaftsklauseln finden unabhängig von einer bestimmten Rechtsform sowohl bei einem Betrieb des Portals in einer öffentlich-rechtlichen Organisationsform als auch bei einem Betrieb in einer privatrechtlichen Organisationsform mit städtischer Beteiligung Anwendung. Sie begrenzen aber fast durchweg nur eine **wirtschaftliche Betätigung**. Darunter versteht man im Allgemeinen das Herstellen, Anbieten oder Verteilen von Gütern oder Dienstleistungen am Markt, die ihrer Art nach auch von einem Privaten mit der Absicht der Gewinnerzielung erbracht werden können (vgl. z.B. Legaldefinitionen in § 107 Abs. 1 S.2 GO NW, ähnlich § 100 Abs.1 GO Bbg). Daneben werden in der Regel gewisse Bereiche vom Gesetz ausdrücklich als nichtwirtschaftlich privilegiert.
Soweit eine wirtschaftliche Betätigung vorliegt, müssen regelmäßig **drei Voraussetzungen** für ihre Zulässigkeit erfüllt sein:

- Ein **öffentlicher Zweck** rechtfertigt oder erfordert die Betätigung;
- Die Betätigung steht nach Art und Umfang in einem angemessenen Verhältnis zu der **Leistungsfähigkeit** der Gemeinde und zum voraussichtlichen **Bedarf**;
- Der öffentliche Zweck kann nicht besser und wirtschaftlicher (**"einfache Subsidiaritätsklausel"**) bzw. ebenso gut und wirtschaftlich ("**verschärfte Subsidiaritätsklausel")** durch einen anderen erfüllt werden. Die meisten Gemeindeordnungen enthalten die einfache Subsidiaritätsklausel, nur in jenen von Mecklenburg-Vorpommern, Rheinland-Pfalz, Bayern, Brandenburg und Thüringen findet sich die verschärfte. Teilweise werden einige Bereiche (vgl. z.B.: § 107 Abs. 1 Nr. 3 GO NW) oder die kommunale Daseinsvorsorge insgesamt (vgl. z.B. § 71 Abs.1 Nr.4 ThürKO, § 102 Abs. 1 Nr. 3 GO Ba-Wü, Art. 87 Abs. 1 Nr. 4 GO Bay) ausdrücklich vom Anwendungsbereich der Subsidiaritätsklausel ausgenommen.

Im Hinblick auf die Auslegung dieser Voraussetzungen wird den Gemeinden von der verwaltungsgerichtlichen Rechtsprechung regelmäßig ein **weiter Beurteilungsspielraum** zugestanden. Insbesondere die Bestimmung des öffentlichen Zwecks stellt sich faktisch daher als eine Frage sachgerechter Kommunalpolitik dar, deren Beantwortung in starkem Maße von Zweckmäßigkeitserwägungen bestimmt wird. Allerdings sollte die Entscheidung für ein Tätigwerden grundsätzlich unter Angabe von **Gründen nachvollziehbar und transparent** gemacht werden. In einigen Ländern sehen die Gemeindeordnungen sogar vor, dass vor der Entscheidung über ein städtisches Tätigwerden optional ein Markterkundungsverfahren (vgl. z.B. § 71 Abs. 1 Ziff. 4 ThürKO), bzw. verpflichtend eine Marktanalyse (§ 107 Abs. 5 GO NW) durchgeführt, bzw. Vergleichsberechnungen angestellt (§ 100 Abs. 3 Satz 2 GO Bbg) werden.
Soweit die Organisationsform unter Beachtung des Grundsatzes der Wirtschaftlichkeit und Sparsamkeit gewählt wurde (vgl. S. 23), ergeben sich für Art und Umfang der Betätigung im Verhältnis zu Leistungsfähigkeit und Bedarf der Gemeinde regelmäßig keine Probleme.
Die ganz herrschende Meinung lässt auch **Randnutzungen** bei zulässigen öffentlichen Betätigungen zur wirtschaftlichen Ausnutzung freier Kapazitäten zu, selbst wenn diese nicht unmittelbar einem öffentlichen Zweck dienen. Voraussetzung ist allerdings, dass es sich aus Wirtschaftlichkeitsgesichtspunkten nur um kapazitätsauslastende Tätigkeitserweiterungen handelt, denen eine untergeordnete Nebenfunktion zukommt und keine zusätzlichen Kapazitäten aufgebaut werden müssen.
Insgesamt divergieren die einzelnen **Vorgaben** für die Zulässigkeit einer staatlichen Betätigung **in den Gemeindeordnungen**. Im Einzelfall können sich aus den

konkreten landesrechtlichen Vorschriften daher **Abweichungen** von den hier dargestellten Ergebnissen ergeben.
Die Rechtsprechung hat sich mit der Problematik der kommunalwirtschaftsrechtlichen Zulässigkeit von städtischen Internetportalen bisher noch nicht beschäftigt. Im Einzelnen sind die Grenzen, die sich aus den Wirtschaftsklauseln ergeben daher noch unklar. Ist eine Tätigkeit den Kommunen selbst nicht erlaubt oder gibt es erhebliche Zweifel an der Zulässigkeit, besteht die Möglichkeit, ein entsprechendes **fremdes Angebot** in den Auftritt unter „www.stadtname.de" zu **integrieren**, so dass es als Angebot fremder Dienstleistungen zu qualifizieren ist. Die Auswahl der privaten Partner muss dabei grundsätzlich unter dem Gesichtspunkt der Chancengleichheit nach Vergabegrundsätzen erfolgen.
Nach der Rechtsprechung des Bundesgerichtshofes können privatwirtschaftliche Mitbewerber über das Wettbewerbsrecht nicht das „Ob" der wirtschaftlichen Betätigung, also den Marktzutritt der Kommunen verhindern. Wohl aber unterliegt das „Wie" der kommunalen Tätigkeit dem Wettbewerbsrecht, so dass diesbezügliche Verstöße auch von privaten Mitbewerbern gerichtlich geltend gemacht werden können.

2.1.2 Welche Informationsangebote sind zulässig?

Kennzeichen des Angebots von Informationsdienstleistungen (vgl. S. 56) über das städtische Portal ist zum einen die Übernahme von technischen und inhaltlichen Hilfsfunktionen durch die Stadt (technischer "Intermediär") und zum anderen die nutzer- und mehrwertorientierte zentrale Bündelung der regionalen Informationsdienstleistungen. Dabei sind **unterschiedliche Fallgruppen einer Bündelung** und Verselbständigung **zu unterscheiden**. Die **erste Fallgruppe** bildet die ausschließliche Bündelung aller Informationsangebote der Stadtverwaltung durch die Verwaltung selbst auf einem Portal (z.B. „www.stadtname.de"). Für die **zweite Fallgruppe** werden zusätzlich Informationsangebote ausgegliederter und im kommunalen Besitz befindlicher Einrichtungen und Unternehmen auf dem Portal integriert. Bei der **dritten Fallgruppe** wird die Bündelung dieser Informationsangebote organisatorisch verselbständigt. Bei der **vierten Fallgruppe** werden zusätzlich Informationsangebote privater Dritter oder über private Dritte in einzelne Angebote auf dem Portal integriert. Die **fünfte Fallgruppe** bildet schließlich die Bündelung aller regionalen Informationsangebote auf einem zentralen städtischen Portal ab.

Warum sind Informationsangebote über die Verwaltung zulässig?

Zulässig ist grundsätzlich die Bündelung von Informationsangeboten über die Verwaltung und von ausgegliederten im kommunalen Besitz befindlicher Einrichtungen und Unternehmen.

Bei der Bündelung der **Informationsangebote über die Stadtverwaltung** (z.B. Öffnungszeiten der Ämter, Informationen über beizubringende Unterlagen, Informationen über Gemeinderatstätigkeit, Selbstdarstellung der Stadt), die sie bei der Erfüllung ihrer Aufgaben unmittelbar unterstützen **(1. Fallgruppe)** liegt schon keine wirtschaftliche Betätigung vor. Die Informationsangebote, die die Verwaltungstätigkeit unmittelbar unterstützen, werden regelmäßig nicht als Tätigkeit "am Markt" angesehen. Ferner verfolgt die hier nur über das neue Medium wahrgenommene Öffentlichkeitsarbeit einen öffentlichen Zweck.
Zulässig ist auch die Integration von **Informationsangeboten über ausgegliederte im kommunalen Besitz befindliche Einrichtungen und Unternehmen (2. Fallgruppe)**. Dazu gehören z.B. die Integration von Informationen städtischer Theater, Informationen zum öffentlichen Personennahverkehr, Informationen zu öffentlichen Bibliotheken und Informationen zu Volkshochschulen. Handelt es sich um bloße **Eigenbedarfsdeckung**

Abbildung 1: Zulässigkeit von Informationsangeboten

Wirtschaftsklauseln in den Gemeindeordnungen			**Fallgruppen der Bündelung von Informationen auf dem Portal**					
			Fallgruppe 1 Ausschließliche Bündelung von Informationsangeboten der Stadtverwaltung durch die Stadt selbst	Fallgruppe 2 Zusätzliche Integration von Informationsangeboten ausgegliederter Einrichtungen und Unternehmen	Fallgruppe 3 Organisatorische Verselbständigung d. gebündelten Angebote d. Fallgruppen 1 u. 2	Fallgruppe 4 Zusätzliche Integration von Informationsangeboten privater Dritter oder über private Dritte Traditionelle Daseinsvorsorgebereiche z.B. Kultur, Soziales, Sport	Sonstige Dienstleister und Wirtschaftsunternehmen	Fallgruppe 5 Bündelung aller regionalen Informationsangebote auf einem städtischen Portal
Keine Anwendbarkeit / ausdrückliche Privilegierung			○	○	○			
Zulässigkeitsvoraussetzungen	Wirtschaftliche Betätigung					○	○	○
	Öffentlicher Zweck					○	○	○
	Leistungsfähigkeit und Bedarf					○	○	○
	Subsidiaritätsklausel	Privilegierung Daseinsvorsorge				○	●	●
		„Einfache" Subsidiaritätsklausel				●	●	●
		"Verschärfte" Subsidiaritätsklausel				●	●	●

○	●
regelmäßige Erfüllung	Einzelfallprüfung

liegt mangels Tätigkeit am Markt regelmäßig schon keine wirtschaftliche Betätigung vor.

- An der Zulässigkeit ändert sich auch nichts, soweit die Betätigung in Form eines Hilfsbetriebes (z.B. Eigenbetrieb, Eigengesellschaft) verselbständigt wurde (3. Fallgruppe). Teilweise wird in den Gemeindeordnungen aber auch schon ausdrücklich eine verselbständigte Bündelung von inhaltlichen und technischen Hilfstätigkeiten, die ausschließlich den gemeindlichen Eigenbedarf decken, als nichtwirtschaftliche Betätigung privilegiert.

Was ist bei der Integration von privaten Informationen im Bereich der Daseinsvorsorge zu beachten?

Werden private Informationsangebote im Sinne der **4. Fallgruppe** im Rahmen von Rubriken integriert, die zu den traditionellen Daseinsvorsorgebereichen gehören (z.B. **Kultur**, **Soziales** und **Sport** bei Veranstaltungskalendern, Vereinsregistern), liegt jedenfalls regelmäßig ein **öffentlicher Zweck** vor (z.B. ein kulturfördernder Zweck durch die Erhaltung des Interesses und der Teilhabe der Einwohner am kulturellen Leben). Einige Stimmen gehen auch bereits davon aus, dass - soweit in den Gemeindeordnungen enthalten- eine Privilegierung als nichtwirtschaftliche Einrichtungen auf den Gebieten Erziehung, Bildung, Kultur, Soziales, Sport und Erholung angenommen werden kann. Allerdings ist diese Einordnung zweifelhaft, da es sich hier nur um inhaltliche und technische Hilfstätigkeiten für reale Einrichtungen handelt und diese Hilfstätigkeiten nur für die Eigenbedarfsdeckung als nicht wirtschaftlich eingeordnet sind.
Mit Blick auf die Subsidiaritätsklausel ist zu unterscheiden: Soweit die **Subsidiaritätsklausel** ausdrücklich den Bereich der **Daseinsvorsorge privilegiert**, sind auf dieser Ebene auch unterstützende Hilfstätigkeiten davon umfasst, so dass die Einbindung Dritter in diesen Bereichen grundsätzlich zulässig ist. Soweit die **„einfache" Subsidiaritätsklausel** Anwendung findet, ist ebenfalls von einer Zulässigkeit auszugehen, wenn keine Anhaltspunkte bestehen, dass Private die Leistungen wirtschaftlicher oder besser erfüllen können. Soweit allerdings die **"verschärfte" Subsidiaritätsklausel** Anwendung findet, ist die Zulässigkeit problematisch. Es kommt auf eine Betrachtung des Einzelfalles an, warum die öffentliche Hand die Aktivitäten besser oder wirtschaftlicher erfüllen kann. Für eine **Rechtfertigung** sind bei der Abwägung insbesondere folgende bedarfsorientierte **Kriterien** einzubeziehen:

- **Strukturelle Rahmenbedingungen** der Gemeinde (z.B. Sozialstruktur der Einwohner; Bedarf an kultureller, sozialer, sportlicher Förderung);
- bestehende oder potenzielle **vergleichbare Angebote** auf dem Markt **Auswirkungen auf die regionale Wirtschaft,** Vorgaben des Mittelstandsförderungsgesetzes;
- **Dauerhaftigkeit** und **Zuverlässigkeit** der Leistungserbringung.

Von einer Zulässigkeit ist auszugehen, wenn nicht ausreichend vergleichbare Angebote auf dem Markt bestehen bzw. diese auch nicht zu erwarten sind und/oder die Angebote den daseinsvorsorgeorientierten Bedarf der Einwohner im Sinne einer gleichmäßigen und dauerhaften Versorgung nicht gleichwertig befriedigen können bzw. könnten.

Was ist bei der Integration von sonstigen Dienstleistern und Wirtschaftsunternehmen zu beachten?

Werden **Informationen über sonstige Dienstleister und Wirtschaftsunternehmen** (z.B. Branchenverzeichnis) oder für den Bereich Tourismus (z.B. Hotel- und Gaststättenführer) integriert (**4. Fallgruppe)**, handelt es sich um eine **wirtschaftliche Betätigung**.
Ein **öffentlicher Zweck** wird für diese Angebote regelmäßig in der kommunalen Wirtschaftsförderung (z.B. Standortförderung, Bestandspflege) gesehen. Zudem wird vielfach hervorgehoben, dass die Internetpräsenz der regionalen Unternehmen für diese zunehmend eine existenzielle Bedeutung einnimmt, um sich in vollem Umfang am wirtschaftlichen Leben beteiligen zu können.
Entscheidende Bedeutung kommt wiederum einer Rechtfertigung unter Hinzuziehung der konkreten Subsidiaritätsklauseln zu. Soweit die **Subsidiaritätsklausel** ausdrücklich den Bereich der **Daseinsvorsorge privilegiert**, ist umstritten, ob die Wirtschaftsförderung als infrastrukturfördernde Maßnahme ebenfalls zum Bereich der Daseinsvorsorge zählt. Anhaltspunkte kann die konkrete Gesetzesbegründung zu den entsprechenden Subsidiaritätsklauseln geben. Soweit die **„einfache" Subsidiaritätsklausel** Anwendung findet, ist von einer Zulässigkeit auszugehen, wenn keine Anhaltspunkte bestehen, dass Private die Leistungen wirtschaftlicher oder besser erfüllen können. Soweit die **„verschärfte" Subsidiaritätsklausel** Anwendung findet, ist die Zulässigkeit problematisch. Es kommt auf eine Betrachtung des Einzelfalles an, warum die öffentliche Hand die Aktivitäten besser oder wirtschaftlicher erfüllen kann. Für eine Rechtfertigung sind bei der Abwägung die bereits oben benannten Kriterien hinzuzuziehen. Als strukturelle Rahmenbedingungen der Gemeinde sind dabei insbesondere auch die Wirtschaftsstruktur zu berücksichtigen. Von einer Zulässigkeit ist dann z.B. auszugehen, wenn es sich um eine strukturschwache Region handelt und nicht ausreichend vergleichbare Angebote auf dem Markt bestehen, über die sich die regionale Wirtschafts- und Touristikunternehmen dauerhaft präsentieren können und der Aufbau eines solchen Angebots auch nicht zu erwarten ist.

Was ist bei der zentralen Bündelung aller regionalen Informationsdienstleistungen zu beachten?

Soweit entsprechend der **5. Fallgruppe** die **Bündelung aller regionalen Informationsdienstleistungen** über ein zentrales Portal angestrebt wird, ist die Zulässigkeit ebenfalls nicht eindeutig. Ein **öffentlicher Zweck** könnte unter Berücksichtigung der verschiedenen einzeln verfolgten öffentlichen Zwecke in der lokalen, dem Handlungsraum des Bürgers entsprechenden Bündelung gesehen werden, die in der von Unübersichtlichkeit geprägten Portallandschaft immer wichtiger werden und zusätzlich in der Sicherstellung der breiten Teilhabe der Bürger über einen diskriminierungsfreien Zugang zu den Informationen. Regelmäßig soll das Abbild der realen Stadt im Netz der Gefahr entgegenwirken, dass das herkömmliche Stadtbild im neuen Strukturgefüge des Internet verschwindet.
Für eine Rechtfertigung im Rahmen der **Subsidiaritätsklauseln** sind bei der Abwägung die bereits für die einzelnen Angebote benannten bedarfsorientierten Kriterien einzubeziehen. Soweit sich aber schon im Rahmen der einzelnen Informationsrubriken eine Legitimation des städtischen Angebots ergeben hat (vgl. S. 17), dürfte **auch die Bündelung** aller regionalen Informationsangebote **zulässig sein**. Eine eindeutige Rechtslage besteht aber noch nicht. Regelmäßig wird eine Einzelfallprüfung notwendig sein.

2.1.3 Welche Kommunikationsangebote sind zulässig?

Zulässig sind Kommunikationsangebote (vgl. näher S. 59), die sich unmittelbar auf die Aufgaben der Verwaltung beziehen (z.B. Beteiligung am Planfeststellungsverfahren, Beteiligung an Rechtsetzungsverfahren). Die Verwaltung unterstützt damit ihre originären staatlichen Aufgaben und handelt nicht wirtschaftlich.
Die Zulässigkeit bedarf aber näherer Prüfung, wenn:

- das Kommunikationsangebot **keinerlei spezifischen Bezug mehr zu den Aufgaben der Verwaltung aufweist** (z.B. allgemeines Chatforum). Für eine Rechtfertigung ist dann zu unterscheiden: Soweit in einigen Gemeindeordnungen Einrichtungen auf den Gebieten **Kultur, Bildung** und **Soziales** als nicht wirtschaftlich privilegiert werden, dürfte eine Einordnung als eine solche privilegierte Einrichtung nahe liegen. Soweit dies nicht der Fall ist, kann für die rechtliche Einordnung auf die Ausführungen zu Informationsangeboten in diesen traditionellen Bereichen der Daseinsvorsorge verwiesen werden (vgl. S. 17);
- ihm eine **meinungsbildende Relevanz** zukommt. Das Angebot darf keinesfalls rundfunkähnlichen Charakter haben. Solange das Angebot aber nicht rundfunkähnlich wird, sondern z.B. aus moderierten Chatforen (vgl. zu Chatforen auch S. 63) besteht, ist verfassungsrechtlich nicht von einer grundsätzlichen Unzulässigkeit wegen des in Art. 5 Abs. 1 Grundgesetz (GG) verankerten Gebots staatsferner, gesellschaftlicher Willensbildung auszugehen. Im Vordergrund steht hier vielmehr die organisatorische Ausgestaltung solcher Angebote der Verwaltung im Sinne einer Neutralitätssicherung der Moderation.

2.1.4 Welche Transaktionsangebote sind zulässig?

Zulässig ist das Angebot aller Transaktionen (vgl. zu Transaktionsangeboten näher S. 65), die die **Aufgaben der Verwaltung** und ihrer ausgelagerten kommunalen Einrichtungen und Unternehmen unterstützen. Insofern handelt es sich lediglich um eine dem technischen Wandel angepasste neue Form der Leistungsabwicklung. Sie stellt grundsätzlich keine wirtschaftliche Betätigung dar.
Soweit auch **private Dienstleister** Transaktionen über das Portal abwickeln wollen, ist die Verwaltung nicht selbst Anbieter dieser Transaktionen, sondern stellt allenfalls Mehrwertdienste bereit, um eine Transaktionsabwicklung zwischen Anbieter und Abnehmer zu erleichtern (z.B. Verschlüsselungsdienste, Paymentserver). Im Hinblick auf die Zulässigkeit des Angebots solcher Mehrwertdienste vgl S. 18.

2.1.5 Sind Mehrwertdienste zulässig?

Zulässig sind Mehrwertdienste (z.B. Paymentserver, Verschlüsselungsdienste, Ausgabe von E-Mails z.B. Name@stadtname.de), die ausschließlich für die Gemeinde selbst und ihre ausgegliederten Einrichtungen zur Verfügung gestellt werden.
Die **Zulässigkeit bedarf näherer Prüfung**, soweit diese Mehrwertdienste auch Dritten zur Verfügung gestellt werden. Ein Angebot ist nur dann als nicht wirtschaftlich und

deshalb bereits zulässig zu qualifizieren, wenn es ausschließlich den Bedarf der Gemeinde selbst und ausgegliederter gemeindlicher Einrichtungen und Unternehmen befriedigt. Hier kann **nicht** von einer **zulässigen Randnutzung** ausgegangen werden, soweit das Angebot solcher Mehrwertdienste vom Umfang grundsätzlich nicht nur vorhandene, sondern auch neue Kapazitäten bindet. Es ist schon **nicht eindeutig**, ob diese Dienste durch einen **öffentlichen Zweck** legitimiert sind. Unzulässig wäre, den öffentlichen Zweck nur in der Einnahmeerzielung über Entgelte oder Provisionen zu sehen (z.B. Provision für jede Transaktion bei Nutzung des Payment-Servers). Es muss also ein anderer Zweck vorliegen, warum das Angebot dieser Dienstleistungen dem Wohl der Gemeinde dient. Für das Angebot von technischen Mehrwertdiensten für private Dienstleister wird dieser in der kommunalen Wirtschaftsförderung gesehen. Für das Angebot von E-Mail-Diensten wird der öffentliche Zweck teilweise mit der Förderung des Internet und bildungspolitischen Aspekten begründet. Nahe liegender ist allerdings, den öffentlichen Zweck in der Stärkung der Identifikation mit der Gemeinde zu sehen.
Mit Blick auf die **Subsidiaritätsklausel** bedarf es einer gesonderten Rechtfertigung**.** Für die Kriterien kann auf die Ausführungen zum Angebot von Informationsdienstleistungen unter Integration sonstiger Dienstleister und Wirtschaftsunternehmen Bezug genommen werden (vgl. S. 17). Berücksichtigt werden müssen auch die Auswirkungen auf privatwirtschaftliche Anbieter solcher Dienste. Die Rechtfertigung der Ausgabe von **E-Mails** dürfte vor dem Hintergrund des großen Angebots an kostenlosen E-Mail-Accounts **problematisch** sein. Im Hinblick auf die **sonstigen technischen Mehrwertdienste** kann **insbesondere in strukturschwachen Städten** unter bestimmten Voraussetzungen von einer **Zulässigkeit ausgegangen** werden. Dies ist z.B. der Fall, wenn nicht ausreichend vergleichbare andere regionale Portale auf dem Markt bestehen, auf die die regionalen Anbieter für die Abwicklung von Transaktionen über das Internet zurückgreifen können und ein solches Angebot in naher Zukunft auch nicht zu erwarten ist.

2.1.6 Ist Werbung auf den Portalseiten zulässig?

Eine wichtige Frage ist, inwieweit die Kommunen über den Verkauf von Werbeflächen auf den Portalseiten Einnahmen erzielen können. Grundsätzlich sind den Kommunen zwar alle Betätigungen verwehrt, die der ausschließlichen Erzielung von Einnahmen dienen, ohne dass ein öffentlicher Zweck gegeben ist. **Zulässig** sind aber **Randnutzungen**, soweit es sich aus Wirtschaftlichkeitsgesichtspunkten nur um kapazitätsauslastende Tätigkeitserweiterungen handelt, denen eine untergeordnete Nebenfunktion zukommt und keine zusätzlichen Kapazitäten aufgebaut werden müssen. Dies gilt selbst dann, wenn diese nicht unmittelbar einem öffentlichen Zweck dienen.
Der Verkauf von Werbeflächen kann grundsätzlich solchen zulässigen Randnutzungen zugeordnet werden, da ihm eine untergeordnete Nebenfunktion zukommt. Es sind aber auch Wettbewerbswirkungen zu berücksichtigen sowie der Grundsatz, dass die öffentliche Wirtschaftstätigkeit privatwirtschaftliches Engagement nicht erdrosseln und den Bestand des Wettbewerbs nicht gefährden darf. Im Hinblick auf das „Wie" der Integration der Werbung ist neben dem Wettbewerbsrecht - soweit es sich um Mediendienste handelt - dann insbesondere das Trennungsgebot des § 13 Mediendienstestaatsvertrag (MDStV) zu beachten.

2.1.7 Unter welchen Voraussetzungen können überregionale private Angebote integriert werden?

Zulässig ist die **punktuelle und untergeordnete Einbindung** von einzelnen Angeboten aus benachbarten Kommunen (z.B. Theaterplan).
Unzulässig ist aber die **umfassende Präsentation** von Anbietern aus fremden Kommunen auf dem Portal, um das Stadtportal gezielt über den gemeindlichen Wirkungsbereich zu erweitern und auch Fremdeinwohner als Zielgruppe anzusprechen ("überregionaler Marktplatz"). Eine **räumliche Beschränkung** des Wirkungsfeldes der Gemeinden ergibt sich aus der verfassungsrechtlichen Begrenzung des kommunalen Selbstverwaltungsrechts (Art. 28 Abs. 2 GG) auf die „Angelegenheiten der örtlichen Gemeinschaft". Sinn und Zweck der "Wirtschaftsklauseln" ist es, die Gemeinden vor einer überdehnten -dem Bedarf und der Leistungsfähigkeit der Gemeinde nicht mehr entsprechenden- unternehmerischen Tätigkeit zu schützen. Vordergründiges Ziel muss daher bei jeder Handlung sein, die speziellen Bedürfnisse und Interessen der Gemeindeeinwohner zu befriedigen.

Weiterführende Literatur und Rechtsprechung:
Zur Anwendbarkeit des § 1 UWG: *BGH*, NVwZ 2002, S. 1141. Allgemein zu den Voraussetzungen der Wirtschaftsklauseln: *Schink*, Wirtschaftliche Betätigung kommunaler Unternehmen, NVwZ 2002, S. 129ff. Zur Zulässigkeit von Kommunen im Internet: *Holznagel/Temme*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 1999, Teil 26 Kommunen im Internet; *Erhard*, Die Zulässigkeit kommunaler Internetaktivitäten, 2002. Zur Zulässigkeit von Werbung: *Kittler*, Die öffentliche Hand als Werbeträger im Internet, NJW 2000, S. 122ff.; *BGH*, GRUR 1973, S. 530. Zur Zulässigkeit von meinungsbildungsrelevanten Angeboten: *Ladeur*, Verfassungsrechtliche Fragen regierungsamtlicher Öffentlichkeitsarbeit und öffentlicher Wirtschaftstätigkeit im Internet, DÖV 2002, S. 1ff. Zur örtlichen Begrenzung: *Gern*, Wirtschaftliche Betätigung der Gemeinden außerhalb des Gemeindegebiets, NJW 2002, S. 2593ff; *Kühling*, Verfassungs- und kommunalrechtliche Probleme grenzüberschreitender Wirtschaftsbetätigung der Gemeinden, NJW 2001, S. 177ff.

2.2 Kann die Verwaltung selbst Aufgaben nach SigG/ SigV wahrnehmen?

§ 4 Abs. 5 Signaturgesetz (SigG) ermöglicht es der Verwaltung als **Registrierungsstelle** aufzutreten. Nach dieser Vorschrift können Zertifizierungsdiensteanbieter Aufgaben an Dritte übertragen, wenn sie diese in ihr gesetzeskonformes Sicherheitskonzept einbeziehen. Dritte im Sinne der Vorschrift sind hierbei alle, die Teilaufgaben übernehmen können, also auch Behörden.

Die Verwaltung könnte nach dem SigG sogar als Zertifizierungsdienstleister tätig werden: Denn auch wenn SigG und SigV grundsätzlich von einer privatwirtschaftlichen Erbringung der Zertifizierung durch private Dienstleister ausgehen (**Marktmodell**), enthalten sie keine Vorgaben, die diese Tätigkeit öffentlichen Stellen ausdrücklich verwehren würden. Praktisch käme aber wohl allenfalls in Betracht, dass die Stadt für ihre eigenen Bedürfnisse als Zertifizierungsdiensteanbieter tätig wird ("Mitarbeitersignaturen"). Aufgrund des technischen und wirtschaftlichen Aufwandes dürfte darüber hinaus wohl nur ein sog. **„virtuelles Trustcenter"** in Betracht kommen, das unter dem Namen der Behörde tätig, technisch aber von einem Dritten betrieben wird.

Soweit die Verwaltung solche Tätigkeiten aufnimmt, muss sie aber auch die Vorschriften des Kommunalwirtschaftsrechts beachten. Hier entsprechen die Grenzen der Zulässigkeit im Ausgangspunkt denen für Mehrwertdienste auf den Portalen (vgl. S. 18). Als legitimierender öffentlicher Zweck ist aber ergänzend auch die Förderung der Online-Kommunikation mit der Gemeinde zu berücksichtigen. Dazu gehört insbesondere auch die Möglichkeit, gegenüber den Bürgern auf geeignete Angaben in den Zertifikaten hinzuweisen (vgl. dazu näher S. 85).

3. Organisationsformen für städtische Portale

Teil einer **Gesamtstrategie** muss auch die Wahl einer geeigneten und ggf. verselbständigten Organisationsform sein. Dabei geht es um die Frage der organisatorischen Ausgestaltung der Gesamtverantwortlichkeit für den Aufbau und Betrieb des Online-Gesamtangebots, unabhängig davon, wer die Aufgaben letztlich tatsächlich ausführt ("make or buy"). Die Verantwortlichkeit umfasst dabei regelmäßig neben dem Betrieb des Portals auch den Aufbau der notwendigen technischen Infrastruktur (technische Plattform).

Als Ausgangspunkt stehen Städten für den Betrieb ihrer Internetportale (als Teil der Leistungsverwaltung) **unterschiedliche rechtliche Formentypen** des öffentlichen und des privaten Rechts zur Verfügung unter denen sie im Rahmen ihrer Selbstverwaltung **grundsätzlich frei wählen** können. In Betracht kommt der Betrieb in öffentlich-rechtlicher Organisationsform (vgl. S. 24), in privatrechtlicher Organisationsform mit kommunaler Beteiligung (vgl. S. 24), ein vollständig privater Betrieb (vgl. S. 32) oder eine Organisationsform unter Berücksichtigung interkommunaler Zusammenarbeit (vgl. S. 34).

Die Wahl des konkreten Organisationsmodells hängt von **Zweckmäßigkeits- und Rechtsmäßigkeitserwägungen** ab.

Im Rahmen der **Zweckmäßigkeitserwägungen ist** zunächst über die strategische Ausrichtung des Portals zu entscheiden. Grundsätzlich kommen zwei **strategische Grundtypen** in Frage: Die "virtuelle Stadt" oder die Beschränkung auf das "virtuelle Rathaus":

- Bei der **„virtuellen Stadt"** soll ein zentrales Portal (i.d.R. „www.stadtname.de") die gesamte „virtuelle Stadt" abbilden und damit nutzerorientiert als Zugang zu sämtlichen öffentlichen, privaten und non-profit-Dienstleistungen der Stadt fungieren.
- Bei dem **„virtuellen Rathaus"** beschränkt sich die Verantwortlichkeit der Stadt bewusst auf Angebote der Verwaltung und kommunaler Einrichtungen.

Wenn das von der Stadt betriebene Portal nur dem Eigenbedarf der Stadt und kommunaler Einrichtungen als Präsentationsplattform dienen soll, kommt auch eine öffentlich-rechtliche Organisationsform in Betracht. **Je stärker aber eine ganzheitliche Lösung** unter Integration Privater im Vordergrund steht, um so mehr liegt die **Verselbständigung** des Betriebs des Portals in einer privatrechtlichen Organisationsform ggf. unter Einbindung Privater bzw. einen vollständig privaten Betrieb.

Aufgrund der sehr unterschiedlichen Ausgangsbedingungen (Größe, Umfeld, Wirtschaftsstruktur) bei Kommunen und Städten kommt es für die Wahl der geeigneten Organisationsform immer auf eine konkrete **Betrachtung des Einzelfalles** an.

Im Rahmen der **Zweckmäßigkeitserwägungen** sind insbesondere folgende Gesichtspunkte beachtlich:

- **Finanzielle Ressourcen**: Dabei spricht die Finanzknappheit tendenziell für die Einbindung Privater bzw. eine vollständige Privatisierung oder für eine interkommunale Zusammenarbeit;
- **Steuerungsmöglichkeiten**: Sie sprechen tendenziell bei einem reinen Verwaltungsbetrieb für eine öffentlich-rechtliche Organisationsform und bei der Einbeziehung Privater für eine Organisationsform mit Beteiligung der Verwaltung;
- **Flexibilität**: Sie spricht tendenziell für private Organisationsformen;
- **Image/Politik**: Diese Motive können mit unterschiedlicher Zielrichtung eingesetzt werden.

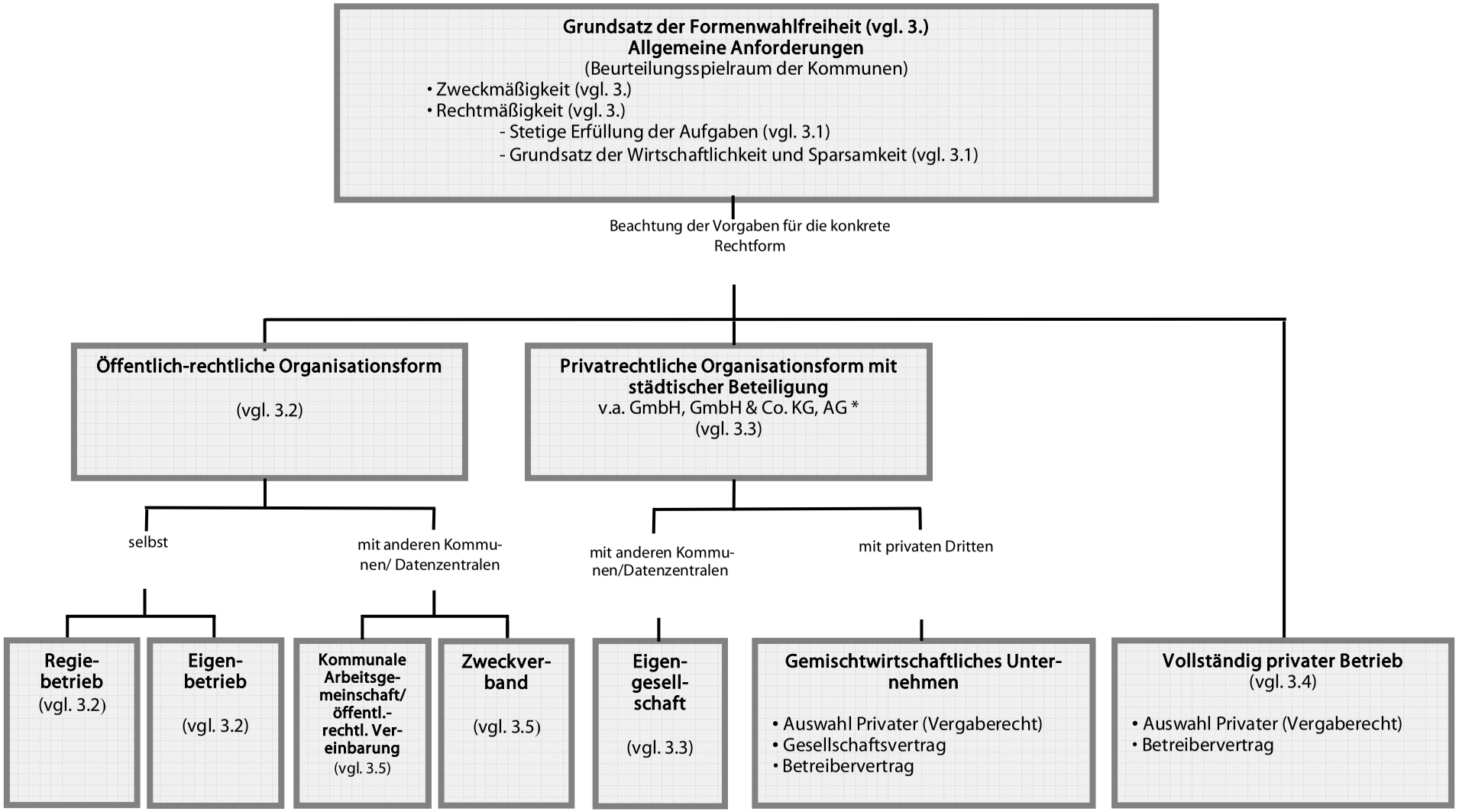
Spezifische politische, verwaltungswissenschaftliche und betriebswirtschaftliche Zweckmäßigkeitserwägungen werden im Folgenden nur soweit berücksichtigt, wie sie rechtlich relevant sind.

Maßstab der hier allein behandelten **Rechtmäßigkeitserwägungen** sind insbesondere die Gemeindeordnungen und spezielle weitere Landesgesetze, die neben allgemeinen Vorgaben vor allem des Gesellschafts- und Vergaberechts zu berücksichtigen sind.

Dabei ist zu beachten, dass das **Landesrecht** zum Teil stark divergiert und an dieser Stelle nicht auf alle Besonderheiten eingegangen werden kann. Die folgende Darstellung ermöglicht aber eine Grundorientierung. Für den konkreten Einzelfall sind immer die speziellen landesrechtlichen Vorschriften hinzuzuziehen.

Weiterführende Literatur:
Allgemein zur Organisation kommunaler Aufgaben: *Henneke* (Hrsg.), Organisation kommunaler Aufgabenerfüllung, 1998. Zur Organisation der virtuellen Stadt: *Eifert/Stapel-Schulz*, Organisation der virtuellen Stadt in Public Private Partnership, ZögU 2002, S. 277ff.
Praxisbeispiele:
Für die unterschiedlichen Konzepte der virtuellen Stadt und des virtuellen Rathauses vgl. *Stapel-Schulz/Eifert* (Hrsg.), Organisations- und Kooperationstypen kommunaler Internetauftritte, Arbeitspapier aus der Begleitforschung zum Städtewettbewerb Multimedia MEDIA@Komm, S. 16ff. (abzurufen unter www.mediakomm.net).

Abbildung 2: Wahl einer Organisationsform



* Sonderform Verein (vgl. 3.3.2)

3.1 Welche allgemeinen Grundsätze sind bei der Auswahl einer Organisationsform zu beachten?

Kommunen haben bei der Organisationswahl **allgemeine Rechtspflichten** zu beachten. Für die Länder sind die Vorgaben in den jeweiligen Haushaltsordnungen der Länder und für die kommunale Ebene durch zahlreiche Vorschriften in den Gemeindeordnungen und Gemeindehaushaltsverordnungen der Länder konkretisiert. Sie lassen sich aber auch verfassungsrechtlich zurückführen.

Bei allen Handlungen und damit auch bei der Auswahl zwischen verschiedenen Handlungs- und Finanzierungsalternativen müssen sich Städte und Kommunen an den **Grundsatz der Wirtschaftlichkeit und Sparsamkeit** halten. Dieser Grundsatz gibt vor, dass auch im Rahmen von Organisationswahlentscheidungen die jeweils günstigste Relation zwischen dem verfolgten Zweck und den eingesetzten Mitteln anzustreben ist. Es ist also diejenige Organisationsform zu wählen, die bei geringstem Aufwand den größtmöglichen Erfolg verspricht (Wirtschaftlichkeit) oder jedenfalls den angestrebten Erfolg mit dem relativ geringsten Aufwand erzielt (Sparsamkeit). Neben der Auswahl einer konkreten Organisationsform ist dabei insbesondere für kleine und wirtschaftsschwache Kommunen auch die Möglichkeit einer interkommunalen Zusammenarbeit einzubeziehen.

Darüber hinaus muss außerdem beachtet werden, dass die Aktivitäten so zu planen sind, dass eine **stetige Erfüllung der Aufgaben** gesichert ist (z.B. Art. 61 Abs.1 GO Bay, § 77 Abs.1 GO Ba-Wü; §109 GO NW). Die Haushaltsgrundsätze setzen somit eine vorausschauende, an der Leistungsfähigkeit und dem Bedarf der Gemeinde orientierte Planung voraus. Bei einem Betrieb in öffentlich-rechtlicher Organisationsform kann selbst für eine dauerhafte Leistungsfähigkeit gesorgt werden, bei einem Betrieb mit privater Beteiligung (vgl. S. 24) oder einem vollständig privatem Betrieb (vgl. S. 32) ist die dauerhafte Leistungserbringung durch vertragliche Instrumente besonders sicherzustellen (vgl. S. 30 und S. 31 bzw. S. 33).

Als Grundlage einer objektiven Beurteilung dienen grundsätzlich im Vorwege durchgeführte angemessene **Wirtschaftlichkeitsuntersuchungen** (vgl. §§ 6 Abs.2 HGrG, 7 Abs. 2 BHO/LHO). In einigen Gemeindeordnungen wird dies näher präzisiert, in dem sie die ausdrückliche Pflicht enthalten, Vergleichsberechnungen vorzunehmen (z.B. § 100 Abs. 3 GO Bbg), bzw. eine Analyse über die Vor- und Nachteile der öffentlichen und der privatrechtlichen Organisationsform für den konkreten Einzelfall zu erstellen. Dabei sind z.B. die organisatorischen, personalwirtschaftlichen, mitbestimmungs- und gleichstellungsrechtlichen sowie die wirtschaftlichen, finanziellen, haftungsrechtlichen und steuerlichen Unterschiede und die Auswirkungen auf den kommunalen Haushalt sowie die Entgeltgestaltung gegenüberzustellen (vgl. z.B. § 123 GO LSA, § 92 Abs.1 GO Rh-Pf).

Teilweise enthalten die Gemeindeordnungen aber auch weitere konkrete Vorgaben, die im Hinblick auf den Abwägungsvorgang zu berücksichtigen sind. So werden in einigen Ländern beispielsweise an die Wahl einer privaten Rechtsform zusätzliche Voraussetzungen gekoppelt und die Gründung eines privaten Unternehmens darf nur erfolgen, wenn sich unter Abwägung der Vor- und Nachteile die Aufgabenerfüllung im Gegensatz zu sonstigen Organisationsformen des öffentlichen Rechts (z.B. Eigenbetrieb) als wirtschaftlicher (§ 109 Abs.1 Nr.1 NGO) bzw. besser (§ 73 Abs.1 Nr.2 ThürKO, § 117 Abs.1 Nr.1 GO LSA) darstellt.

Im Hinblick auf das Abwägungsergebnis kommt den Städten und Gemeinden grundsätzlich ein Beurteilungsspielraum zu, so dass in das Ergebnis immer auch z.B. planerische, finanzpolitische und sonstige Erwägungen der Zweckmäßigkeit einfließen können. Wegen der großen Unsicherheiten über die Entwicklung des Internetsektors ist regelmäßig ein weiter Beurteilungsspielraum anzunehmen.

Die Entscheidung über die Verselbständigung des Betriebs des Portals und die nähere Art und Ausgestaltung der Organisationsform bedarf grundsätzlich **eines Beschlusses durch den Gemeinderat**. Grundlage des Beschlusses ist entsprechend der konkreten kommunalwirtschaftlichen Vorgaben eine an den örtlichen Bedürfnissen und der Leistungsfähigkeit der Gemeinde ausgerichtete Begründung, warum die konkrete Organisationsform gewählt wurde. Ferner ist die **Aufsichtsbehörde** einzubeziehen. Soweit vor der Entscheidung des Gemeinderates ausdrücklich die Erstellung einer Analyse vorgesehen ist, muss diese der Aufsichtsbehörde vor der Entscheidung des Gemeinderats vorgelegt werden (vgl. z.B. § 123 Abs.1 S.3 GO LSA, § 92 Abs.1 S.2 GO Rh-Pf; § 102 SächsGemO). Ansonsten ist die Entscheidung des Gemeinderats vor Vollzug der Maßnahme der Aufsichtsbehörde anzuzeigen. (vgl. z.B. § 115 GO NW).

Weiterführende Literatur:
Gern, Deutsches Kommunalrecht, 2. Aufl. 1997, Rnr. 659ff.

3.2 Was ist bei einer öffentlich-rechtlichen Organisationsform zu bedenken?

Soweit sich die Stadt für eine öffentlich-rechtliche Organisationsform entscheidet, stehen als unselbständige öffentlich-rechtliche Organisationsformen insbesondere die Formen des Eigenbetriebs und des Regiebetriebs zur Verfügung. Sie bringen ein unterschiedliches Maß an relativer rechtlicher Verselbständigung zum Ausdruck.

Der **Regiebetrieb** ist derjenige Organisationstyp, der sich am engsten an die Gemeindeverwaltung anlehnt. Für ihn existieren keine speziellen Vorgaben, sondern es gelten die allgemeinen gemeinderechtlichen Bestimmungen. Regiebetriebe eignen sich primär, um den gemeindlichen Eigenbedarf zu befriedigen und kommen wohl nur bei einem reinen Verwaltungsportal in Betracht.

Der **Eigenbetrieb** stellt die Normalform des unselbständigen wirtschaftlichen Unternehmens der Kommune dar. Er bietet als ebenfalls rechtlich unselbständige Organisationsform den Vorteil, einer wirtschaftlichen Betriebsführung bei gleichzeitiger bestehender Einfluss- und Steuerungsmöglichkeiten durch Rat und Verwaltung der Gemeinde. Die städtischen Portalaktivitäten erfüllen die prinzipielle Voraussetzung für die Gründung eines Eigenbetriebes, da sie auf einen dauerhaften Betrieb gerichtet sind und nach Art und Umfang der Tätigkeit eine selbständige Wirtschaftsführung rechtfertigen.

Nähere Vorgaben für die Gründung und Ausgestaltung des Eigenbetriebs ergeben sich aus dem speziellen Eigenbetriebsrecht.

Im Einzelfall können die Gemeindeordnungen weitere **Sonderformen** vorsehen, wie z.B. in Bayern die weitergehende Verselbständigung in Form des selbständigen Kommunalunternehmens als Anstalt des öffentlichen Rechts (vgl. nähere Vorgaben in Art. 89 ff. GO Bay).

Weiterführende Literatur:
Cronauge, Kommunale Unternehmen, 4. Aufl. 2002; *Gern*, Kommunalrecht, 2. Aufl. 1997, Rnr. 741 ff; *Zeiß*, Das Recht der gemeindlichen Eigenbetriebe, 4. Aufl. 1993.
Praxisbeispiel für einen Eigenbetrieb:
Hagener Betrieb für Informationstechnologie (HABIT), vgl. http://vrhagen.stadt-hagen.de.

3.3 Was ist bei einer privatrechtlichen Organisationsform mit städtischer Beteiligung zu bedenken?

Entscheidet sich die Stadt für einen privaten Betrieb, kommt für die Organisation des Internetportals aufgrund der in den Gemeindeordnungen enthaltenen zwingenden Haftungsbegrenzung regelmäßig nur eine **GmbH, GmbH&Co. KG oder AG** in Betracht. Nur als Sonderfall kann bei nichtwirtschaftlicher Ausrichtung des Portals und zur Einbindung Dritter auch die Gründung eines gemeinnützigen Vereins erwägenswert sein (vgl. näher S. 32).

Erforderlich ist damit regelmäßig die **Gründung einer privatrechtlichen Gesellschaft** und die Übertragung der städtischen Domain auf die Gesellschaft, meist im Rahmen eines gesonderten Betreibervertrags. Die näheren Gestaltungsmöglichkeiten richten sich nach den jeweiligen allgemeinen gesellschaftsrechtlichen Vorgaben. Hieraus ergibt sich auch der Vorteil der GmbH und GmbH&Co. KG gegenüber einer Aktiengesellschaft, der in der leichteren Gründung und der flexibleren Sicherstellung der Einflussrechte der Gemeinde besteht. Aufgrund ihrer Praxisrelevanz beziehen sich die folgenden Ausführungen daher ausschließlich auf die GmbH und GmbH&Co.

Ist die Stadt alleiniger Träger der Gesellschaft, spricht man von einer **Eigengesellschaft.** Allerdings spielen im Rahmen der Portaltätigkeiten der Städte aufgrund der eigenen Ressourcenknappheit weniger Eigengesellschaften, als vielmehr Beteiligungsgesellschaften unter Einbindung Privater (**gemischtwirtschaftliche Unternehmen**) eine Rolle. Für beide Gesellschaftstypen enthalten die Gemeindeordnungen grundsätzlich dieselben speziellen Vorgaben, die im Folgenden behandelt werden.

3.3.1 Was ist bei der Gründung eines gemischt wirtschaftlichen Unternehmens zu beden ken?

Von einem **gemischtwirtschaftlichen Unternehmen** wird gesprochen, wenn an einer Gesellschaft sowohl die öffentliche Hand als auch Private beteiligt sind. Aus Sicht der öffentlichen Hand ist diese Option interessant, da insbesondere privates Kapital und Know How mit eingebunden werden kann und die feste gesellschaftsrechtliche Verbindung über einen langen Zeitraum Planungssicherheit bringt.

Es existieren grundsätzlich keine Vorgaben, wie hoch der **Anteil der öffentlichen Hand** an dem Unternehmen sein muss. Vielmehr sind auch Minderheitsbeteiligungen zulässig. Allerdings müssen dabei die sich für die kommunale Ebene aus den Gemeindeordnungen ergebenden Pflichten zur angemessenen Einflusssicherung beachtet werden. Dabei sind insbesondere die Schwellen des gesellschaftsrechtlichen Minderheitenschutzes zu berücksichtigen.
Private Akteure halten bei einem gemischtwirtschaftlichen Unternehmen aus steuerlichen Gründen teilweise die **Rechtsform der GmbH&Co. KG** im Vergleich zu einer GmbH für attraktiver. Sie erlaubt es den privaten Partnern zunächst zu erwartende Verluste mit anderweitig anfallenden Gewinnen zu verrechnen und so Steuervorteile zu erzielen.

Was ist bei der Auswahl der privaten Partner zu beachten?

Entscheidet sich die Kommune für einen Betrieb des Portals in der Rechtsform eines gemischtwirtschaftlichen Unternehmens, müssen in einem ersten Schritt geeignete private Partner gefunden werden. Solche Partner können aus vielfältigen Branchen kommen (z.B. IT-Dienstleister, Kreditinstitute, Presseunternehmen). Für die Auswahl ist das **Vergaberecht** zu berücksichtigen.

Wann ist Vergaberecht anzuwenden?

Das Vergaberecht bezweckt bei einem **Beschaffungsvorgang der öffentlichen Hand** aus Gründen der Chancengerechtigkeit die Auswahl der privaten Partner unter Beachtung von Wettbewerbs- und insbesondere Preisgesichtspunkten.
Der Anwendungsbereich des Vergaberechts erstreckt sich auf **öffentliche Aufträge**, d.h. entgeltliche Verträge der öffentlichen Hand, die Liefer-, Bau- oder Dienstleistungen zum Gegenstand haben (vgl. auch § 99 GWB). Insgesamt bestehen im Hinblick auf die Reichweite und Vorgaben des Vergaberechts mangels gefestigter Rechtsprechung noch **große Unsicherheiten**, so dass es immer auf eine Betrachtung des Einzelfalles ankommt. Da eine Verletzung des Vergaberechts in der Regel die Nichtigkeit des Vertrages mit sich bringt, sollte daher **in Zweifelsfällen** immer das **Vergaberecht beachtet** werden.
Betrachtet man ausschließlich die **Gründung des gemischtwirtschaftlichen Unternehmens** selbst, so fehlt es grundsätzlich an einem öffentlichen Auftrag in Form eines "Beschaffungsvorgangs" und damit an einer Anwendbarkeit des Vergaberechts. Wird das gemischtwirtschaftliche Unternehmen aber als Mittel gegründet, um diesem den Betrieb des Portals zu übertragen und die Gründung mit einer konkreten Auftragserteilung verknüpft, kommt eine Anwendbarkeit des Vergaberechts grundsätzlich in Betracht kommt.

Wann kann eine Ausnahme von der Anwendbarkeit des Vergaberechts vorliegen?

Ausnahmen von der Anwendbarkeit des Vergaberechts können sich nur dann ergeben wenn es sich um ein so genanntes "Inhouse-Geschäft" handelt oder die Einordnung als eine so genannte Dienstleistungskonzession nahe liegt.

- Von einem **Inhouse-Geschäft** spricht man, wenn die Stadt über die beauftragte Gesellschaft eine Kontrolle
- ausübt und die Gesellschaft quasi als „Dienststelle" des öffentlichen Auftraggebers anzusehen ist, so dass die Beauftragung damit einem internen Organisationsakt gleicht. Bei welcher Beteiligungshöhe der öffentlichen Hand an dem gemischtwirtschaftlichen Unternehmen dies der Fall ist und wie die Kontrollrechte dafür im Einzelnen ausgestaltet sein müssen, bedarf einer Betrachtung des Einzelfalls. In jedem Fall muss eine sehr enge Anbindung bestehen. In Zweifelsfällen ist eine Anwendbarkeit des Vergaberechts anzuerkennen.
- Die Übertragung des Internetportal-Betriebs auf das gemischtwirtschaftliche Unternehmen verbindet in der Regel das Angebot der Verwaltung an das private Unternehmen, die ihr zugeordnete Domain (i.d.R. „www.stadtname.de") zu nutzen mit dessen Verpflichtung, festgelegte gemeinwohlorientierte Leistungen zu erbringen. Dies legt eine Einordnung als eine so genannte Dienstleistungskonzession nahe, die bei der Erfüllung einer im Allgemeininteresse liegenden Aufgabe nach überwiegender Ansicht nicht unter das Vergaberecht fällt. Hier übernimmt der Betreiber die Leistungen grundsätzlich in eigener Verantwortung und auf eigenes wirtschaftliches Risiko, ohne dass er ein direktes Entgelt vom öffentlichen Auftraggeber erhält. Dabei ist eine teilweise Gegenleistung, die hier in der Domain-Übertragung besteht, grundsätzlich unschädlich. Steht allerdings die Domain-Vergabe als Preis der Verwaltung im Vordergrund oder sind von der Verwaltung zusätzliche Entgelte zu entrichten, so ist das Vergaberecht anzuwenden. In Zweifelsfällen

sollte wiederum das Vergaberecht Anwendung finden. Auch bei Abschluss von Verträgen, die eine Dienstleistungskonzession zum Gegenstand haben, muss die Vergabe im Übrigen in nicht-diskriminierender und transparenter Form erfolgen.

Was ist bei der Organisation des Vergabeverfahrens zu bedenken?

Das Vergabeverfahren ist ein komplexer Vorgang, der die Stadt in ihren Kompetenzen ggf. überfordert. In diesen Fällen ist die Unterstützung durch einen (externen) Fachspezialisten ratsam und zulässig. Nach der gängigen Rechtsprechung muss bei der **Hilfe durch sachkundige Dritte** aber gewährleistet sein, dass es sich letztlich weiter um eine eigenverantwortliche Entscheidung des öffentlichen Auftraggebers handelt und der Dritte weder unmittelbar noch mittelbar ein eigenes Interesse am Ergebnis des Vergabeverfahrens hat.
Soweit externer privater Sachverstand (z.B. durch eine Consulting-Firma) hinzugezogen werden soll, ist eine Anwendbarkeit des Vergaberechts auf die Unterstützungsleistung grundsätzlich gegeben und damit in der Regel eine Ausschreibung zur Ausschreibung erforderlich (vgl. zur sog. „Bagatellbeschaffung“ S. 26).
Soweit Unternehmen für den Auftraggeber vor Einleitung des Vergabeverfahrens bereits Vorarbeiten geleistet haben, ist eine Beteiligung dieser sog. **Projektanten** im anschließenden Vergabeverfahren problematisch. Ein Ausschluss vom Wettbewerb eines solchen Unternehmens kommt in Betracht, wenn dem Unternehmen durch die Beteiligung an Planungs- und sonstigen Vorarbeiten Kenntnisse zugewachsen sind, die ihm einen Wettbewerbsvorsprung vor seinen Wettbewerbern sichern. Es ist aber möglich, Informationsvorsprünge abzubauen, in dem die Verdingungsunterlagen einschließlich der Leistungsbeschreibung so gestaltet werden, dass die im Rahmen der Vorbereitung erlangten Kenntnisse allen zugänglich gemacht werden.
Soweit **Mitarbeiter der Kommune** oder Stadt mit der Ausschreibung betraut werden, ist unter Berücksichtigung des Gleichbehandlungsgrundsatzes und Neutralitätsgebots sicherzustellen, dass bei ihnen **kein Interessenkonflikt** besteht (vgl. auch § 16 Vergabeverordnung (VgV).

Welche vergaberechtlichen Vorgaben sind zu beachten?

Soweit das Vergaberecht Anwendung findet, muss zunächst geklärt werden, welche vergaberechtlichen Vorgaben Anwendung finden. Dabei ist nach dem **Schwellenwert des Auftrags** zu unterscheiden. In der Regel wird es sich bei der Beauftragung eines gemischtwirtschaftlichen Unternehmens mit dem Betrieb des Portals um ein Leistungsvolumen oberhalb des Schwellenwertes in Höhe von **Euro 200.000** handeln (für den niedrigeren Schwellenwert bei Aufträgen des Bundes vgl. § 2 Nr. 2 VgV. Anwendbar ist dann der 4. Teil des Gesetzes gegen Wettbewerbsbeschränkungen (GWB), die VgV und der 2. Abschnitt der Verdingungsordnung für Leistungen –ausgenommen Bauleistungen Teil A (VOL/A). Es bedarf danach einer europaweiten Ausschreibung im Amtsblatt der Europäischen Gemeinschaften.
Soweit es sich im Einzelfall doch um ein Auftragsvolumen **unterhalb dieses Schwellenwertes** handelt (z.B. bei der Ausschreibung zur Ausschreibung), bleiben die **allgemeinen haushaltsrechtlichen Bestimmungen** anwendbar. So bestimmt § 30 des Haushaltsgrundsätzegesetzes: ”Dem Abschluss von Verträgen über Lieferungen und Leistungen muss eine öffentliche Ausschreibung vorausgehen, sofern nicht die Natur des Geschäfts oder besondere Umstände eine Ausnahme rechtfertigen.” Entsprechende Bestimmungen finden sich in den Haushaltsordnungen der Gemeinden (z.B. § 31 der GemHVO NW, § 31 GemHVO Ba-Wü, § 29 GemHVO M-V). Eine Anwendbarkeit der VOL/A ergibt sich hier nur, soweit Land und Kommunen durch haushaltsrechtliche Vorschriften zur Anwendung verpflichtet sind. Auf Landesebene liegen entsprechende Erlasse vor, während für die kommunale Ebene die VOL/A teilweise ausdrücklich für anwendbar erklärt worden sind (vgl. § 29 GmHVO M-V), teilweise aber auch nicht. Allerdings haben auch viele Gemeinden durch innerdienstliche Anweisungen selbst sichergestellt, dass die VOL/A bei der Vergabe berücksichtigt wird. Für einen öffentlichen Auftrag unterhalb des Schwellenwertes reicht eine nationale Ausschreibung.

Welche Verfahrensart des Vergaberechts ist anzuwenden?

Das Vergaberecht unterscheidet zwischen dem offenen, nicht offenen und Verhandlungsverfahren. Das **offene Verfahren** richtet sich an eine unbeschränkte Zahl von Unternehmen und stellt aus Wettbewerbsgesichtspunkten den **Grundsatz** dar. Es kann nur dann umgangen werden, wenn ein Ausnahmetatbestand die Anwendbarkeit einer

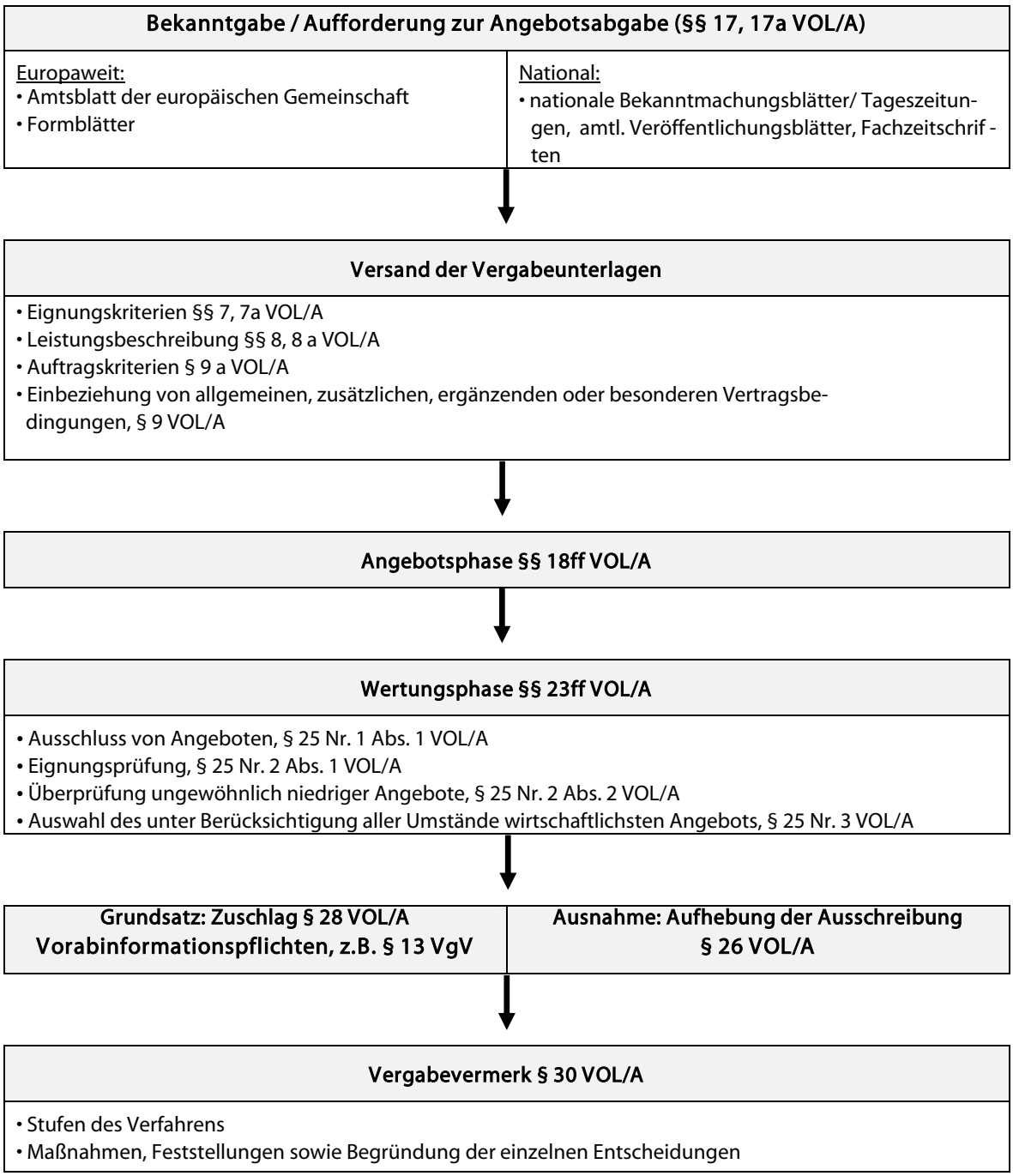
anderen Verfahrensart zulässt. Soweit die Kommune oder Stadt daher von diesem Verfahren abweichen will, sollte sie sich intensiv mit der Anwendbarkeit der Verfahrensart beschäftigt haben und im Falle des Abweichens vom offenen Verfahren darlegen, auf welchen Ausnahmetatbestand sie sich dabei stützt. Teilweise enthalten auch spezielle Verwaltungsvorschriften die ausdrückliche Pflicht, alle maßgeblichen Gründe aktenkundig festzuhalten (vgl. auch § 30 VOL/A).

Ausnahmen vom offenen Verfahren kommen nur in eng begrenzten Fällen in Betracht. Dazu zählen insbesondere:

- sog. **Bagatellbeschaffungen:** Hier kann das Verhandlungsverfahren auf Grundlage von § 3 Nr. 4 Buchst. p VOL/A durch Ausführungsbestimmungen bis zu einem bestimmten Höchstwert ausdrücklich zugelassen sein. Dieser Höchstwert kann insbesondere bei einer Ausschreibung zur Ausschreibung unterschritten sein;
- eine **Unmöglichkeit der eindeutigen und erschöpfenden Leistungsbeschreibung:** Lassen sich die genauen Modalitäten und Leistungen der Partnerschaft noch nicht beschreiben und können hinreichend vergleichbare Angebote nicht erwartet werden, ist es vergaberechtlich zulässig, ein Verhandlungsverfahren durchzuführen (§§ 3 Nr. 4 h), 3 a Abs.4 b) und c) VOL/A). Diese Ausnahmen können für Aufbau und Betrieb der Internetportale und -plattformen häufig vorliegen, wenn im Planungsstadium die Inhalte und Leitbilder, die mit der „virtuellen Stadt" und ihrer Realisierung durch das Portal verbunden werden, zunächst nur als Politikziele umrissen werden können und sich damit eine eindeutige und erschöpfende Leistungsbeschreibung als unmöglich darstellt. Aus Gründen der Chancengleichheit ist es aber dennoch geboten, eine öffentliche Aufforderung voranzustellen, sich um Teilnahme zu bewerben (§ 3 Nr.1 Abs. 4 VOL/A).
- Beim **Verhandlungsverfahren** ist die Kommune/Stadt nur begrenzt an formelle Vorschriften gebunden. Insbesondere kann sie mit dem Bieter über Inhalt und Preise des Angebots verhandeln.

Weiterführende Literatur und Rechtsprechung:
Allgemein zu den vergaberechtlichen Vorgaben und Verfahrensarten: *Ax/Schneider/Nette*, Handbuch Vergaberecht, 2002; *Hertwig*, Praxis der öffentlichen Auftragsvergabe: VOB/VOL/VOF, 2. Aufl., 2001. Zur Anwendbarkeit von Vergaberecht bei Gründung eines gemischtwirtschaftlichen Unternehmens: *Dreher*, Public Private Partnerships und Kartellvergaberecht, NZBau 2002, S. 245ff.; *Jaeger*, Public Private Partnership und Vergaberecht, NZBau 2001, S. 6ff.. Zur Einordnung als Inhouse-Geschäft: *Faber*, Öffentliche Aufträge an kommunalbeherrschte Unternehmen - in house-Geschäfte oder Vergabe im Wettbewerb?, DVBl. 2001, S. 248ff.; *EuGH*, NZBau 2000, S. 90; *VK Düsseldorf*, NZBau 2001, S. 46. Zur Dienstleistungskonzession: *Schreiben der EG-Kommission* zu Auslegungsfragen im Konzessionsbereich, NZBau 2000, S. 413; *BayOLG*, NZBau 2002, S. 233; *OLG Naumburg*, NZBau 2002, S. 235. Zur Transparenzpflicht bei Dienstleistungskonzessionen: *EuGH*, NZBau 2001, S. 148. Zur Einschaltung von Dritten im Rahmen des Vergabeverfahrens: *OLG Düsseldorf, NZBau 2001, S. 155, OLG Rostock NZBau 2000. S- 479: Vergabekammerdes Bundeskartellamts, Beschluss vom 14.7.2000, VK 2-16/00*

Abbildung 3: Das Vergabeverfahren – Übersicht


Bekanntgabe / Aufforderung zur Angebotsabgabe (§§ 17, 17a VOL/A)
Europaweit:
• Amtsblatt der europäischen Gemeinschaft
• Formblätter
National:
• nationale Bekanntmachungsblätter/ Tageszeitungen, amtl. Veröffentlichungsblätter, Fachzeitschriften
Versand der Vergabeunterlagen
• Eignungskriterien §§ 7, 7a VOL/A
• Leistungsbeschreibung §§ 8, 8 a VOL/A
• Auftragskriterien § 9 a VOL/A
• Einbeziehung von allgemeinen, zusätzlichen, ergänzenden oder besonderen Vertragsbedingungen, § 9 VOL/A
Angebotsphase §§ 18ff VOL/A
Wertungsphase §§ 23ff VOL/A
• Ausschluss von Angeboten, § 25 Nr. 1 Abs. 1 VOL/A
• Eignungsprüfung, § 25 Nr. 2 Abs. 1 VOL/A
• Überprüfung ungewöhnlich niedriger Angebote, § 25 Nr. 2 Abs. 2 VOL/A
• Auswahl des unter Berücksichtigung aller Umstände wirtschaftlichsten Angebots, § 25 Nr. 3 VOL/A
Grundsatz: Zuschlag § 28 VOL/A
Vorabinformationspflichten, z.B. § 13 VgV
Ausnahme: Aufhebung der Ausschreibung
§ 26 VOL/A
Vergabevermerk § 30 VOL/A
• Stufen des Verfahrens
• Maßnahmen, Feststellungen sowie Begründung der einzelnen Entscheidungen

Was ist bei der Gründung der GmbH und GmbH&Co.KG zu bedenken?

Aufgrund der Komplexität der Vertragsgestaltung ist im Anschluss an die Auswahl der privaten Partner ratsam, zunächst in Form eines **„letter of intent"** die Absicht der Zusammenarbeit mit ihren wesentlichen Parametern festzuhalten. Für die folgende Gründung der GmbH ist ein **Gesellschaftsvertrag** erforderlich. Er wird regelmäßig durch einen **Betreibervertrag** ergänzt.
Der Gesellschaftsvertrag wird im Handelsregister publiziert und ist daher öffentlich zugänglich. Soweit ein Bedürfnis besteht, bestimmte sensible Vertragsinhalte nicht in dem Gesellschaftsvertrag öffentlich zu machen (z.B. Regelungen zur Finanzierung), können diese auch in einer zusätzlichen Vereinbarung der Gesellschafter **(Konsortialvertrag)** getroffen werden.

Kann die städtische Domain eine Einlage bilden?

Neben einer Kapitaleinlage kommt als mögliche Einlage der Stadt in die Gesellschaft auch eine **Sacheinlage** in Form der Übertragung des Nutzungsrechts an der städtischen Domain in Betracht. Für den Fall der Auflösung der Gesellschaft ist dann aber in jedem Fall auch vertraglich die **Rückübertragung des Nutzungsrechts** vorzusehen. Bei einer Sacheinlage müssen allerdings Leistungsgegenstand und die Bemessung seiner Höhe präzise im Gesellschaftsvertrag niedergelegt sein (§§ 5 IV, 19 V GmbHG).
Problematisch ist die **Bemessung des Wertes der Domain**. Einen Orientierungspunkt können dabei die Grundsätze für die Bemessung von Streitwerten bei Domainstreitigkeiten bieten. Für die konkrete Bemessung des Wertes der Domain sollte abhängig vom Nutzungszweck ihr Gebrauchswert im Vordergrund stehen. Dieser bestimmt sich u.a. über die Größe und Bekanntheit der Stadt, die Zugriffszahlen und die über das Portal zu erwartenden Gewinne.

Mit welchen Mitteln kann die Stadt ihre Kontroll- und Einflusspflichten wahrnehmen?

Die Gemeindeordnungen enthalten Vorgaben, um den städtischen Einfluss auch bei privatrechtlichen Organisationsformen sicherzustellen und die Zielvorgaben des Unternehmens zu gewährleisten.
Der mit dem Unternehmen verfolgte öffentliche Zweck (vgl. auch S. 14) muss im Gesellschaftsvertrag festgeschrieben werden.

Um die öffentliche Zwecksetzung zu garantieren, müssen nach den Gemeindeordnungen außerdem angemessene **Einwirkungs-, Beteiligungs-, Mitsprache- und Kontrollrechte der Gemeinde** durch die Satzung festgelegt werden. Welcher Einfluss angemessen ist, ist eine Frage des Einzelfalles und bestimmt sich u.a. nach der Bedeutung des verfolgten öffentlichen Zwecks.
Einflussmöglichkeiten ergeben sich aufgrund der Gesellschafterstellung der Stadt durch die Vertretung in der Gesellschafterversammlung durch den Bürgermeister bzw. einen von ihm bestimmten Vertreter. Die von der Gemeinde entsandten Mitglieder in Gremien der Gesellschaft können die besonderen Interessen der Gemeinde einbeziehen.
Die Flexibilität der Organisation der GmbH erlaubt darüber hinaus über den Gesellschaftervertrag den Belangen der einzelnen Gesellschafter weiter Rechnung zu tragen (§ 45 GmbHG). Insbesondere folgende **Regelungselemente sind im Gesellschaftsvertrag** zur Einflusssicherung der Städte möglich:

- Die Gemeinde hat das Recht, den Geschäftsführer zu bestellen und abzuberufen.
- Das Stimmgewicht der Gesellschafter wird abweichend von § 47 GmbHG (Einflussmöglichkeiten richten sich nach der Höhe der Kapitalbeteiligung) geregelt, bzw. gewisse Entscheidungen der Gesellschaftsversammlung werden von der Zustimmung der Gemeinde abhängig gemacht (z.B. Verkauf von Anteilen der privaten Gesellschafter).
- Es werden Weisungsrechte der Gesellschafter oder des Aufsichtsrats an die Geschäftsführung bei laufenden Geschäften vorgesehen.
- Es wird ein Vorkaufsrecht der Gemeinde bei Veräußerung von Geschäftsanteilen eines Mitgesellschafters vorgesehen.

Es wird die Berechtigung der Übernahme von Anteilen eines Mitgesellschafters eingeräumt, falls sich dessen eigene Beteiligungsstruktur in einer Weise ändert, die die Erfüllung der öffentlichen Aufgaben gefährdet.
Daneben kann auch eine weitergehende vertragliche Präzisierung der Einflussmöglichkeiten über die Festlegung von Pflichten im Betreibervertrag erfolgen (vgl. S. 31).
Rechtlich vorgeschrieben ist außerdem die Einflusssicherung durch die **Gründung eines Aufsichtsrates**, bzw. entsprechenden Überwachungsorgans. Weiter ist zu beachten, dass die einzelnen Gemeindeordnungen teilweise darüber hinausgehende ausdrückliche Pflichtvorgaben enthalten,

die mittels Gesellschaftsvertrag abgesichert werden müssen (vgl. z.B. § 103a GO Ba-Wü).
Es ist schließlich zu beachten, dass eine „Beherrschung" im Sinne des Konzernrechts wegen der Haftungsfolgen unterbleibt.

Was ist im Betreibervertrag zu regeln?

In einem Betreibervertrag können die gegenseitigen Pflichten der Beauftragung und weitere konkrete Parameter der Vertragsbeziehung niedergelegt werden. Empfehlenswert ist, hier nochmals die von dem Unternehmen einzuhaltenden öffentlichen Zwecke zu präzisieren.
Als **Pflichten auf Betreiberseite kommen** insbesondere in Betracht:

- Aufbau einer technischen Infrastruktur für das Angebot von Information, Kommunikation und Transaktionsdienstleistungen ggf. mit Einbindung der elektronischen Signatur und eines Bezahlservers;
- Verpflichtung auf eine State-of-the-Art-Technologie;
- Einhaltung der Vorgaben für die Gestaltung des Portals („Styleguide");
- Unterstützung bei Migration der Daten;
- Gewährleistung eines störungsfreien Betriebs;
- Gewährleistung des kostenlosen Einstellens von Verwaltungsinhalten.; Gewährleistung eines bestimmten (kostenlosen bzw. kostengünstigen) Angebots von Dienstleistungen (z.B. kostenloser Grundeintrag für Firmen) im Rahmen der öffentlichen Zwecksetzung;
- Gewährleistung eines diskriminierungsfreien Zugangs zum Portal;
- Einhaltung der Datenschutzbestimmungen (vgl. S. 35);
- Festlegung von Meilensteinen und Fristen;
- Hilfsfunktionen des virtuellen Rathauses (z.B. Bearbeitung und Weiterleitung von Eingängen über das Portal; Betrieb von Postfächern für die Empfänger von Nachrichten der Gemeinde).

Als **Pflichten auf Seiten der Stadt kommen** insbesondere in Betracht:

- Kooperation/Beteiligung bei der Entwicklung von neuen technischen Anwendungen an der Schnittstelle zur Verwaltung;
- ggf. Zahlung eines bestimmten Entgelts für die Inanspruchnahme von Leistungen;
- Soweit die Domain nicht schon als Sacheinlage in das Gesellschaftsvermögen eingeht: Übertragung des Nutzungsrechts an der städtischen Domain auf die private Gesellschaft;
- Garantie, dem Betreiber die (redaktionell bearbeiteten) Verwaltungsinhalte bereitzustellen und Verwaltungstransaktionen über das Portal abzuwickeln;
- ggf. exklusive Überlassung der Verwaltungsinhalte (vgl. zur Zulässigkeit von Exklusivvereinbarungen S. 33).

Als allgemeine **sonstige Inhalte** kommen insbesondere in Betracht:

- Dauer der Beauftragung;
- Kündigung/Beendigung des Vertrages;
- Rückübertragung des Nutzungsrechts an der Domain und Migration der Daten;
- Haftung;
- Streitschlichtungsmechanismus.

Was ist zu beachten, wenn dem gemischtwirtschaftlichen Unternehmen auch Mitarbeiter der Stadt zur Verfügung gestellt werden sollen?

Werden Mitarbeiter der Stadt als **Angestellte des öffentlichen Dienstes** dem gemischtwirtschaftlichen Unternehmen zur Verfügung gestellt, kann dies entweder durch einen Betriebsübergang mit Arbeitgeberwechsel oder im Wege der Personalgestellung/Personalbeistellung ohne Arbeitgeberwechsel geschehen.
Bei einem **Betriebsübergang** tritt nach § 613 a Abs. 1 BGB das gemischtwirtschaftliche Unternehmen als privater Arbeitgeber bei Angestellten des öffentlichen Dienstes grundsätzlich in alle Arbeitsverhältnisse ein. Regelmäßig werden diese Betriebsübergänge durch sog. **Personalüberleitungsverträge** zwischen dem öffentlichen Arbeitgeber und der Gesellschaft unter Wahrung der Beteiligungsrechte der öffentlichen Interessenvertretungen (Personalrat) abgeschlossen. Der bisherige Arbeitnehmer hat die betroffenen Arbeitnehmer z.B. über Zeitpunkt, Grund, Folgen und Maßnahmen zu unterrichten (§ 613 a Abs. 5 BGB). Die vom Betriebsübergang betroffenen Arbeitnehmer haben die Möglichkeit, dem Übergang des Arbeitsverhältnisses auf den neuen Arbeitgeber binnen eines Monats nach Unterrichtung zu widersprechen (§ 613 a Abs. 6 BGB).

Personalgestellungs-/Beistellungsverträge regeln typischerweise die Fortgeltung der Tarifverträge und Dienstvereinbarungen zwischen öffentlichem Arbeitgeber und dem Arbeitnehmer in der jeweils geltenden Fassung. Die Vorgaben des Arbeitnehmerüberlassungsgesetzes (AÜG) sind zu berücksichtigen. Die Zurverfügungstellung von Angestellten der Stadt erfordert nach den Personalvertretungsgesetzen der Länder grundsätzlich die **Beteiligung des Personalrats**. Regelmäßig hat der Personalrat bei der beabsichtigten Maßnahme zumindest mitzuwirken, so dass bestimmte Verfahrensschritte einzuhalten sind (vgl. z.B. Art. 72 des Personalvertretungsgesetzes von Bayern - PersVG Bay). Dazu gehört insbesondere seine frühzeitige Einbindung sowie umfassende und vollständige Unterrichtung.
Die Beschäftigung eines **Beamten** in einem gemischtwirtschaftlichen Unternehmen kann beispielsweise durch eine Dienstleistungsüberlassung, Zuweisung oder durch die Gewährung von Sonderurlaub erfolgen. Für Beamte ist dabei regelmäßig das spezielle Beamtenrecht (z.B. Landesbeamtengesetze, Beamtenrechtsrahmengesetz (BRRG)) zu beachten. Das Personalvertretungsrecht der Länder enthält entsprechende Sondervorschriften für die **Mitwirkung der Personalvertretung**, etwa im Falle der Zuweisung eines Beamten im Sinne von § 123 a Abs. 2 BRRG (vgl. z.B. Art. 75 Abs. 1 Nr. 14 PersVG Bay).

Weiterführende Literatur:
Allgemein zur Gründung eines gemischtwirtschaftlichen Unternehmens: *Schellenberg/Lepique/Fedder/Pape/Moos*, Die Realisierung einer Public Private Partnership durch Gründung eines Kooperationsunternehmens, Verwaltung und Management (VM) Sonderbeilage 4/2002, S. 1ff.. Zur Gründung einer gemischtwirtschaftlichen Betreibergesellschaft für das städtische Portal: *Eifert*, Die rechtliche Sicherung öffentlicher Interessen in Public Private Partnerships - dargestellt am Beispiel der Internet-Aktivitäten von Städten und Kommunen, VerwArch 2002, S. 561ff. ; *Schellenberg*, Die vertragliche Gestaltung einer Public Private Partnership zum Aufbau eines öffentlichen Portals, in: Kröger (Hrsg.), Internetstrategien für Kommunen, 2001, S. 411ff.; Bertelsmann Stiftung (Hrsg.), E-Government finanzieren: Wege zu Public-Private-Partnerships, 2003. Zu arbeitsrechtlichen Fragen: *Schellenberg/Lepique/Fedder/Pape/Moos*, Die Realisierung einer Public Private Partnership durch Gründung eines Kooperationsunternehmens, VM Sonderbeilage 4/2002, S. 1 (7 ff.).
Praxisbeispiele:
Für die Gründung einer gemischtwirtschaftlichen GmbH&Co.KG: Hamburg.de GmbH&Co. KG (www.hamburg.de); Bremen Online Services (www.bremer-online-service.de).

3.3.2 Was ist bei einer Gründung eines Vereins grundsätzlich zu bedenken?

Teilweise werden zur Bündelung und Koordinierung von Vereinsaktivitäten auf dem Portal gezielt Vereine in die Organisationsstruktur eingebunden. Soweit von Seiten der Gemeinde **sozialpolitische Aspekte** bei Betrieb des Portals im Vordergrund stehen und weniger die Rentabilität, bildet die Rechtsform des eingetragenen nichtwirtschaftlichen Vereins auch eine mögliche Organisationsform für den Gesamtauftritt. Traditionelle Bereiche der Aufgabenerfüllung durch eingetragene nichtwirtschaftliche Vereine sind der Kultur, Bildungs- oder Fremdenverkehrssektor. Der Verein ermöglicht die Einbeziehung privater Akteure und die Koordinierung unterschiedlicher Interessen. Er ist aber nur begrenzt auf das Management einer wirtschaftlichen Tätigkeit eingestellt. Nähere Vorgaben zu Gründung und Ausgestaltung des Vereins enthalten die §§ 21 ff. BGB.

Praxisbeispiele:
Für den Einsatz eines Vereins zur Koordination des Auftritts von Vereinen und Foren auf dem Portal: www.muenster.de. Für den Betrieb des Portals in der Organisationsform eines Vereins: www.rathenow.de.

3.4 Was ist bei einem vollständig privaten Betrieb zu bedenken?

Will die Stadt den Betrieb des Portals nicht selbst übernehmen, kann sie auch gezielt einen privaten Betreiber suchen. Dafür wird das Nutzungsrecht an der/einer städtischen Domain auf einen privaten Dritten übertragen, der Aufbau und Betrieb des Portals und der technischen Plattform übernimmt. Die Gemeinwohlinteressen der Kommunen können über einen **Betreibervertrag** abgesichert werden. Auf diesen Vertrag ist ein besonderes Augenmerk zu richten, da er die **einzige Möglichkeit zur Absicherung der Kontroll- und Einflussnahme** der Kommune darstellt.

3.4.1 Was ist bei der Auswahl der privaten Partner zu beachten?

Für die allgemeinen Vorgaben bei der Auswahl der privaten Partner vgl. S. 25. An dieser Stelle werden lediglich Abweichungen und Besonderheiten hervorgehoben. Auch hier liegt eine Einordnung des Kooperationsverhältnisses zwischen der Kommune und den Privaten als eine dem Vergaberecht nicht unterliegende **Dienstleistungskonzession** (vgl. S. 25) nahe, wenn die Stadt nur eine „untergeordnete" Leistung erbringt (i.d.R. Übertragung des Nutzungsrechts an der Domain). Regelmäßig werden private Partner aber aufgrund des zunehmenden Preisverfalls für Domainnamen noch zusätzliche Leistungen von der Stadt verlangen. So-

weit allerdings diese Gegenleistung der Stadt in den Vordergrund rückt und der private Betreiber z.B. von der Stadt zusätzliche Vorrechte (z.B. Exklusivvereinbarungen) oder konkrete Entgelte für bestimmte Dienstleistungen erhält, ist eine Anwendbarkeit des Vergaberechts sachgerecht. In Zweifelsfällen sollte das Vergaberecht angewendet werden. Die Gemeinwohlinteressen und Einflussmöglichkeiten werden über einen Betreibervertrag abgesichert. Dafür werden dem privaten Betreiber gewisse Pflichten auferlegt. Es ist sinnvoll, diese **Pflichten in der Ausschreibung möglichst präzise** darzulegen, damit frühzeitig die Parameter für die Kooperation von Seiten der Stadt gesetzt sind.

3.4.2 Was ist im Betreibervertrag zu regeln ?

Der **Betreibervertrag** regelt die Kooperation zwischen der Kommune und dem grundsätzlich in eigener Verantwortung handelnden Privaten Betreiber des Stadtportals. Er stellt die **einzige Steuerungsmöglichkeit** der Kommune dar und muss aufgrund seiner über die allgemeinen Angelegenheiten der Verwaltung hinausgehende Bedeutung vom **Gemeinderat beschlossen** werden.
Durch den Betreibervertrag wird das Nutzungsrecht an der Domain für einen bestimmten Zeitraum (i.d.R. 5-10 Jahre) auf den privaten Betreiber übertragen, der sich im Gegenzug verpflichtet, ein bestimmtes Angebot unter bestimmten Modalitäten bereitzustellen. Für die grundsätzlichen **Inhalte des Betreibervertrages** vgl. S. 31. Da der Vertrag die einzige Steuerungsmöglichkeit darstellt, sollte darauf geachtet werden, die Vertragsinhalte besonders dezidiert festzulegen, um Unklarheiten und Lücken zu vermeiden und eine dauerhafte Einflusssicherung der Stadt zu gewährleisten.
Zusätzlich sollte darauf geachtet werden, dass insbesondere noch folgende Aspekte im Betreibervertrag geregelt werden:

- **Einflusssicherung durch die Schaffung eines „Abstimmungsgremiums" und Sicherung von Informationsrechten:** Sinnvoll ist die vertragliche Festlegung der Gründung eines Abstimmungsgremiums, welches sich aus Vertretern der Betreibergesellschaft und der Stadt zusammensetzt und regelmäßig Fragen/Probleme des operativen Betriebs abstimmt. Des weiteren sollte sich die Stadt über den Betreibervertrag ein jederzeitiges Informationsrecht sichern;
- **Einflusssicherung bei Gesellschaftswechsel:** Um unerwünschte Teilhaber bei einem Gesellschafterwechsel zu verhindern, ist z.B. die Festlegung eines Vorkaufsrechts der Stadt bei Verkauf von Gesellschaftsanteilen oder eines Kündigungsrechts der Stadt bei Gesellschafterwechsel sinnvoll;
- **Lückenlose Fortführung des Betriebs nach Beendigung des Vertragsverhältnisses:** Es ist zu berücksichtigen, dass der Betreiber nach Ablauf der Vertragslaufzeit, ggf. kein Interesse an einer Fortführung des Betriebs des Portals hat. Um die lückenlose Fortführung des Betriebs durch einen anderen Betreiber oder die Kommune selbst sicherzustellen, sind für diesen Fall vertragliche Vorkehrungen zu treffen, wie z.B. die Gewährleistung der Übertragung des Portals/der Infrastruktur zu einem bestimmten Preis und die frühzeitige Festlegung auf interoperable technische Standards;
- **Vorgaben des Datenschutzes** (vgl. S. 35).

3.4.3 Sind Exklusivvereinbarungen zulässig?

Der private Portalbetreiber wird ein Interesse daran haben, dass die Stadt ihre Verwaltungsinformationen exklusiv an ihn weitergibt und die Verwaltungsdienstleistungen über die Plattform abgewickelt werden. Im Hinblick auf die **wettbewerbsrechtliche Zulässigkeit** solcher Vereinbarungen besteht noch **Unsicherheit**. Das Kammergericht Berlin hat in einer zu www.berlin.de ergangenen Entscheidung die zeitlich exklusive Weitergabe von Informationen der öffentlichen Hand an einen privaten Internetdienst als zulässig angesehen.
Allerdings ist diese Entscheidung nicht verallgemeinerungsfähig. Das Gericht hat die öffentlich-rechtlichen Fragen letztlich offen gelassen, weil es die subjektive Voraussetzung des in Rede stehenden wettbewerbsrechtlichen Anspruchs verneinte. Im Übrigen deutete es die Exklusivvereinbarung so, dass es sich nicht um eine „echte Exklusivität" handele, sondern auch Konkurrenten der zeitnahe Zugriff auf die Informationen nicht gänzlich entzogen sei. Es kommt daher vielmehr immer auf eine **Betrachtung des konkreten Einzelfalls** an. Für die Frage, der Zulässigkeit sollten im Rahmen der Abwägung folgende **Kriterien** berücksichtigt werden:

- Diskriminierungsfreies Auswahlverfahren der Partner;
- Dauer der Exklusivität;
- Umfang der Exklusivität;
- Wirtschaftliches Eigeninteresse der Stadt.

Weiterführende Rechtsprechung und Literatur:
Zu Exklusivvereinbarungen: *KG Berlin*, AfP 2001, S. 519ff.; *Köhler/Piper*, Gesetz gegen den unlauteren Wettbewerb, Kommentar, 3. Aufl. 2002, § 1 Rnr. 544 ff.
Praxisbeispiele:
Für einen vollständig privaten Betrieb: www.berlin.de, www.koeln.de.

3.5 Interkommunale Zusammenarbeit

Vor allem für kleinere Kommunen bietet sich angesichts der Komplexität der Aufgaben und der Ressourcenknappheit eine interkommunale Zusammenarbeit an. Dabei stehen sowohl öffentlich-rechtliche als auch privatrechtliche Möglichkeiten zur Verfügung. Als **öffentlich-rechtliche Formen** kommen insbesondere die in den Gesetzen der Länder über die kommunale Zusammenarbeit (GkomZ) enthaltenen Instrumente der kommunalen Arbeitsgemeinschaft, der öffentlich-rechtlichen Vereinbarung und des Zweckverbandes in Betracht. Als **privatrechtliche Organisationsform** ist insbesondere die Bildung einer GmbH mit gesellschaftlicher Beteiligung mehrerer Kommunen (Eigengesellschaft, vgl. S. 24) zu erwägen.

- **Unverbindliche kommunale Arbeitsgemeinschaften** und **verbindliche öffentlich-rechtliche Vereinbarungen** kommen insbesondere für eine **punktuelle Zusammenarbeit bei einfachen Problemlagen** in Betracht, die bei Betrieb und Aufbau der Plattform auftreten (z.B. für die Bildung von Einkaufsgemeinschaften und den Austausch über technische Lösungen und Standards). Ist eine Verbindlichkeit bei der Wahrnehmung einer konkreten Aufgabe gewollt, ist eine Ausgestaltung der Kooperation in Form einer öffentlich-rechtlichen Vereinbarung sinnvoll.
- Für die gemeinsame Lösung von komplexeren Sachverhalten – wie z.B. die Entwicklung komplexer technischer Lösungen oder den gemeinsamen Aufbau und Betrieb eines Portals- steht die Einrichtung des **Zweckverbandes** zur Verfügung. Zu einem Zweckverband können sich Gemeinden und Landkreise, aber auch andere Körperschaften zusammenschließen. Daneben können auch natürliche und juristische Personen des Privatrechts Mitglied sein, wenn die Erfüllung der Verbandsaufgaben dadurch gefördert wird und Gründe des öffentlichen Wohls nicht entgegen stehen. Da die Mitwirkungsmöglichkeit Privater in einem Zweckverband sich allerdings nur auf untergeordnete Funktionen beschränkt, wird von privater Seite regelmäßig die Organisationsform eines gemischtwirtschaftlichen Unternehmens vorgezogen werden. Auch ist der Zweckverband relativ schwerfällig gegenüber Änderungen der Zusammensetzung und Aufgaben.

Der Zweckverband stellt eine neue juristische Person dar. Die Aufgabe scheidet in vollem Umfang aus dem Zuständigkeitsbereich der bisherigen kommunalen Körperschaft aus und geht auf den Zweckverband über. Nähere Vorgaben zu Aufbau und Ausgestaltung eines Zweckverbandes sind in den GkomZ enthalten. Die Gesetze über die Zusammenarbeit bei der automatisierten Datenverarbeitung legen für den Bereich der automatischen Datenverarbeitung teilweise Abweichungen vom allgemeinen Recht der Zweckverbände fest, um die Nutzung dieser Rechtsform für diese Aufgaben zu erleichtern. Grundsätzlich kann als Hauptzweck eines Zweckverbandes auch der **Betrieb eines wirtschaftlichen Unternehmens** festgelegt werden. Allerdings müssen dann gewisse gesetzlich geregelte Modifikationen beachtet werden.

- Insbesondere wenn es sich um eine Kooperation bei einer wirtschaftlichen Betätigung handelt, hat aufgrund der effizienteren Entscheidungsstruktur die **Bildung einer GmbH** (vgl. S. 24) als **privatrechtliche Organisationsform** Vorteile gegenüber dem Zweckverband.

Wenn im Land etablierte und funktionierende Kooperationsstrukturen für den Bereich der Automatischen Datenverarbeitung bestehen (v.a. Datenzentralen und -verbände), sollten sie berücksichtigt werden. Rechtspflichten zur Zusammenarbeit bestehen hier aber regelmäßig nicht.

Weiterführende Literatur:
Allgemein zu Interkommunaler Zusammenarbeit: *Schink,* Organisationsmodelle für überörtliche Kooperationen, in: Henneke (Hrsg.), Optimale Aufgabenerfüllung im Kreisgebiet?, 1999, S. 61ff.; *KGSt* (Hrsg.), Tul-Leistungserstellung: Interkommunale Zusammenarbeit und Alternativen, KGSt Bericht 13/1996. Zur Rolle von Rechenzentren und Datenzentralen: *Reinermann* (Hrsg.), Regieren und Verwalten im Informationszeitalter, 2000, S. 334 ff.
Praxisbeispiele:
Für Arbeitsgemeinschaften und öffentlich-rechtliche Vereinbarungen: Arbeitsgruppe Internet der Stadt und Kreisverwaltung Wernigerode (vgl. www.wernigerode.de); Projekt Verwaltung 2000 der schleswig-holsteinischen Landkreise, vgl. www.komfit.de/projekte/Vw2000.htm. Für einen interkommunale Eigengesellschaft: Curiavant Internet GmbH für den Städteverbund Nürnberg (www.curiavant.de); die öffentlich-rechtliche Besitzgesellschaft der Projekt Rhur-GmbH, vgl. www.d-nrw.de.

3.6 Was ist aus datenschutzrechtlicher Sicht bei einer Aufgabenübertragung an Dritte zu beachten?

Werden im Rahmen der elektronischen Abwicklung Verwaltungsaufgaben oder einzelne Arbeitsabläufe auf eine andere Stelle übertragen, sind besondere datenschutzrechtliche Bestimmungen zu beachten. Um die datenschutzrechtlichen Ansprüche an eine Zulässigkeit der Datenverarbeitung durch Dritte zu bestimmen, wird zwischen Datenverarbeitung im Auftrag und Datenverarbeitung im Rahmen genereller Funktionsübertragung differenziert. Hiernach bestimmt sich auch, welche Stelle die erforderlichen Maßnahmen zur Datensicherung erbringen muss. Die **Datenschutzbeauftragten führen dazu aus:**

- „(...) Bei der **Auftragsdatenverarbeitung** liegt die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der personenbezogenen Daten beim Auftraggeber, der „Herr" seiner Daten bleibt. Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragnehmer vor. Dem Auftragnehmer wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter materieller Verantwortung des Auftraggebers, gewissermaßen als sein verlängerter Arm, übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine **„Hilfsfunktion"** der eigentlichen Aufgabe ausgelagert, ohne dass der Auftragnehmer einen eigenen Handlungs- oder Entscheidungsspielraum hat."
- „Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Auftragnehmer über die technische Durchführung hinaus materielle Leistungen mit Hilfe der überlassenen Daten oder bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Aufgabe, es liegt eine **Funktionsübertragung** vor. In diesem Fall wird **der Auftragnehmer zur Daten verarbeitenden Stelle** und hat eigenständig für die zur Datensicherung und zur Gewährleistung von Vertraulichkeit erforderlichen technischen und organisatorischen Maßnahmen zu sorgen". Die Übertragung der Aufgaben unterliegt selbstverständlich auch den allgemeinen verwaltungsrechtlichen Grundsätzen.

„Die Bewertung, ob eine Auftragsdatenverarbeitung oder Funktionsübertragung vorliegt, lässt sich nur im **Einzelfall** vornehmen. Deutliche Erkennungsmerkmale bei Auftragsdatenverarbeitung sind die fehlende Entscheidungsbefugnis des Dritten, die weisungsgebundene Unterstützungstätigkeit und die fehlende Beziehung des Dritten zum Betroffenen. Merkmale der Funktionsübertragung sind weiterhin die Überlassung von Nutzungsrechten an den Daten, die eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dritten sowie das Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch).
Besondere Probleme ergeben sich bei Daten, für die besondere Schutzvorschriften bestehen. Durch die Datenweitergabe werden die Daten dem Dritten offenbart. Dies ist unzulässig, wenn der Offenbarung **gesetzliche Schutzvorschriften** entgegenstehen. Dazu gehören insbesondere Berufsgeheimnisse (zum Beispiel das Arztgeheimnis) und besondere Amtsgeheimnisse (wie das Steuergeheimnis). In diesen Fällen ist eine Weitergabe der Daten an Dritte nur zulässig, wenn die betreffenden Schutzvorschriften die Offenbarung dieser Daten erlauben. (...)"
"Beauftragt eine Behörde ein privates Dienstleistungsunternehmen oder einen anderen Dritten, um für sie Hardware, Software oder auch Tele- und Mediendienste zu betreiben und zu warten (Outsourcing), so ist dabei auf folgende Punkte zu achten:

- Der Auftragnehmer sollte kein eigenes, fachlich bestimmtes Interesse an einem Zugriff auf Inhaltsdaten haben (Eingrenzung der Gefahr eines Datenmissbrauches).
- Bereits bei der Auswahl des Auftragnehmers ist darauf zu achten, dass er die erforderlichen technischen und organisatorischen Maßnahmen ergreifen kann. Das setzt voraus, dass alle wesentlichen Anforderungen

bekannt sein müssen und sich der Auftraggeber davon überzeugt hat, dass der Auftragnehmer in der Lage ist, diese umzusetzen, bevor der Auftragnehmer erstmals Gelegenheit erhält, auf personenbezogene Echtdaten zuzugreifen.

- Den Regeln der Auftragsdatenverarbeitung entsprechend, muss für jedes Outsourcing-Vorhaben ein schriftlicher Auftrag erteilt werden. Darin sind Rechte und Pflichten der Daten verarbeitenden Stelle und des Fernwartungsunternehmens detailliert festzulegen; Gegenstand und der Umfang der übertragenen Tätigkeiten; die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Datenschutzmaßnahmen sowie etwaige Unterauftragsverhältnisse darzustellen.
- 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 (z.B. nach § 5 BDSG) zu verpflichten.
- In der Vereinbarung ist ferner festzulegen, dass der Auftragnehmer sich der Kontrolle der zuständigen staatlichen Datenschutzaufsichtsbehörde 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." Vgl. zu Fragen des Datenschutzes bei virtuellen Poststellen S. 50.

4. Einbindung privaten IT- Know Hows

Mit Blick auf den Grundsatz der Wirtschaftlichkeit und Sparsamkeit (vgl. 3.1) ist die Möglichkeit der Einbindung privaten IT-Know Hows zu berücksichtigen. In Betracht kommen der Abschluss von Einzelverträgen über IT- Leistungen, ein umfangreiches Outsourcing oder das Eingehen einer Entwicklungspartnerschaft. Daneben gewinnt auch das **Application Service Providing** (ASP) an Bedeutung. Darunter versteht man ein Dienstleistungskonzept, bei dem Anwendungs- oder Programmfunktionalitäten über das Internet oder andere Netze vermietet werden. Im Hinblick auf die Auswahl privater Partner sind die für IT-Dienstleistungen/Outsourcing dargestellten Vorgaben maßgeblich. Mangels näherer vertraglicher Typisierung, soll diese Art von Dienstleistung hier nicht näher behandelt werden.

4.1 Was ist bei Einzelverträge über IT-Leistungen/Outsourcing zu bedenken?

Einzelverträge über festdefinierte IT-Leistungen zur Einbindung von privatem Know-How können punktuell und in vielfältigen Bereichen abgeschlossen werden. Sie finden auch im E-Government weite Verbreitung. Typische Dienstleistungsarten bilden z.B. die IT-Projektberatung, IT-Schulungen, das Bereitstellen von inhaltsunabhängigen Providerdiensten, die Entwicklung und Pflege von Software, die Instandhaltung von Hardware, die Pflege von Website-Inhalten und sonstige mit der Datenverarbeitung verbundene Dienstleistungen, aber auch die dauerhafte Auslagerung des Server- oder Datenbankbetriebes.

4.1.1 Was ist bei der Auswahl der privaten Partner zu beachten?

Welche vergaberechtlichen Vorgaben sind zu beachten?
Zu den allgemeinen Vorgaben bei der Auswahl privater Partner vgl. S. 25. Für die Bestimmung, welche vergaberechtlichen Bestimmungen der Verdingungsordnungen konkret Anwendung finden, bedarf es einer Betrachtung des Einzelfalles. Grundsätzlich kommen hier die Verdingungsordnung für freiberufliche Leistungen (VOF) und die Verdingungsordnung für Leistungen (VOL/Teil A) in Betracht.
Eine **Anwendbarkeit der VOF** kommt grundsätzlich bei einem Auftragsvolumen oberhalb von 200.000 immer dann in Betracht, wenn es sich um die Vergabe von Leistungen handelt, die im Rahmen einer **freiberuflichen Tätigkeit** erbracht oder im Wettbewerb mit freiberuflichen Tätigkeiten angeboten werden (§ 1 VOF). Hier kommen v.a. ingenieurähnliche Tätigkeiten in Betracht, wie z.B. die Software-Implementierung von Systemsoftware und damit zusammenhängende vorbereitende Tätigkeiten. Für die genaue Abgrenzung kommt es auf eine Betrachtung des **Einzelfalles** an und ob es sich um eine vorab objektiv **nicht eindeutig und erschöpfend beschreibbare** freiberufliche Leistung handelt (§ 2 Abs. 2 Satz 2 VOF).
Die nach **VOF** anzuwendende Vergabeart ist **grundsätzlich das Verhandlungsverfahren** mit vorheriger Vergabebekanntmachung (§ 5 Abs. 1 VOF).
Soweit der Anwendungsbereich der VOF nicht in Betracht kommt, sind für **Dienstleistungen der Datenverarbeitung und verbundene Tätigkeiten** oberhalb des Schwellenwertes grundsätzlich die Bestimmungen des **2. Abschnitts der VOL/A** maßgebend (vgl. Anhang I a, Kategorie 7 der Dienstleistungsrichtlinie). Werden diese Dienstleistungen zusammen mit Lieferleistungen (z.B. Kauf von EDV-Hardware) in Auftrag gegeben, handelt es sich nach § 1 a Nr. 1 Abs. 2 VOL/A immer noch um einen Dienstleistungsauftrag, wenn der Wert der im Auftrag enthaltenen Dienstleistung den Wert des Lieferanteils übersteigt. Bei **IT-Dienstleistungsaufträgen** ist aufgrund des **Vorliegens eines typischen Beschaffungsvorgangs** grundsätzlich das **offene Verfahren** anzuwenden. Nur in engen Ausnahmen ist ein Verhandlungsverfahren, ggf. ohne vorherige Vergabebekanntmachung zulässig. Dies kann in vergröberter Darstellung (!) insbesondere der Fall sein, wenn:

- eine sog. **Bagatellbeschaffung** vorliegt (vgl. S. 26);
- bei zeitlich auf höchstens drei Jahre befristeten **zusätzlichen Lieferungen des ursprünglichen Auftragnehmers** technische Kompatibilität sichergestellt werden soll (vgl. § 3 a Nr. 2 e) VOL/A);
- **zusätzliche IT-Dienstleistungen** wegen eines unvorhergesehenen Ereignisses zur Ausführung des ursprünglichen Vertrages erforderlich sind und besonders eng mit diesem zusammenhängen oder einen vergleichsweise geringen Wert haben (vgl. § 3 a Nr. 2 f) VOL/A);
- **neue IT-Dienstleistungen** in der Wiederholung gleichartiger, in einem Grundentwurf früher bereits ausgeschriebener Leistungen bestehen (vgl. § 3 a Nr. 2 g) VOL/A);
- für die Leistung aus besonderen Gründen (z.B. besondere Erfahrungen, Zuverlässigkeit) nur ein Unternehmen in Betracht kommt (vgl. § 3 Nr. 4 a) VOL/A);

- im Anschluss an Entwicklungsleistungen Aufträge in angemessenem Umfang und für angemessene Zeit an Unternehmen, die an der Entwicklung beteiligt waren, vergeben werden müssen (vgl. § 3 Nr. 4 b) VOL/A).

Insbesondere bei der **Softwarebeschaffung** kann in **Einzelfällen** auch eine **beschränkte Ausschreibung** zulässig sein, wenn die Leistung nach ihrer Eigenart nur von einem beschränkten Kreis von Unternehmen in geeigneter Weise ausgeführt werden kann (vgl. § 3 Nr. 3 a) VOL/A). Bei einer solchen beschränkten Ausschreibung werden Leistungen im vorgeschriebenen Verfahren nach Aufforderung einer beschränkten Zahl von Unternehmen zur Einreichung von Angeboten vergeben.
Im Ergebnis ist also festzuhalten: Soweit es sich bei dem Dienstleistungsauftrag oberhalb von Euro 200.000 um eine nicht eindeutig und erschöpfend beschreibbare „ingenieurähnliche Leistung" handelt, ist das Verhandlungsverfahren zulässig. Ansonsten ist bei der Vergabe von Dienstleistungen im IT-Bereich grundsätzlich das offene Verfahren anzuwenden ist. Ausnahmen bestehen insbesondere für bereits bestehende Vertragsbeziehungen oder wenn die Leistung nur von einem oder mehreren Unternehmen ausgeführt werden kann.

Hat auch der gemischtwirtschaftliche Betreiber Vergaberecht zu beachten?

Auch ein gemischtwirtschaftliches Unternehmen (vgl. S. 24) hat im Rahmen seiner Auftragsvergabe Vergaberecht zu beachten, soweit es als **öffentlicher Auftraggeber im Sinne von § 98 Nr. 2 GWB** anzusehen ist. Dies ist dann der Fall, wenn:

- das Unternehmen im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art zu erfüllen hat **und**
- von der Stadt überwiegend finanziert oder überwiegend geleitet wird.

Dabei ist eine **Betrachtung des Einzelfalls** vorzunehmen. Soweit der Betreiber entsprechend der öffentlichen Zwecksetzung tätig wird, erfüllt er grundsätzlich auch im **Allgemeininteresse** liegende Aufgaben. Das Vorliegen eines entwickelten Wettbewerbs und insbesondere der Umstand, dass das betreffende Unternehmen auf dem jeweiligen Markt im Wettbewerb steht, ist nach Rechtsprechung des Europäischen Gerichtshofs ein geeignetes Auslegungs- und Wertungskriterium zur Bestimmung der Gewerblichkeit bzw. **Nichtgewerblichkeit**. Zu berücksichtigen ist dabei aber auch, ob das Unternehmen einen kommerziellen oder industriellen Charakter hat. Für das Vorliegen der zusätzlichen Voraussetzung bedarf es im Einzelfall einer Betrachtung der Finanzierungs-, Gesellschafts- und Organisationsstruktur des Unternehmens. Im Zweifel ist Vergaberecht anzuwenden.

Was ist beim Abschluss von langfristigen Verträgen zu bedenken?

Insbesondere beim Outsourcing von IT-Dienstleistungen kommt der Abschluss von umfassenden und langfristigen Verträgen in Betracht. Hier treten vergaberechtliche Fragen v.a. hinsichtlich der **Zeitdauer** und der Behandlung der Einzelleistungen unter einem **Rahmenvertrag** auf.
Grundsätzlich ist bei Langfristverträgen in gewissen **zeitlichen Abständen** zu **überprüfen**, ob eine neue Ausschreibung erforderlich ist. In **Einzelfällen** ist bei Vorliegen besonderer Umstände (z.B. Aufbau eines umfangreichen DV-Konzeptes, grundlegende technische Veränderungen) die Bindung über einen längeren Zeitraum zulässig. Soweit ein Vertrag mit einer **automatischen Verlängerungsklausel** abgeschlossen wird, ist die Verlängerung des Vertrages nur der Ausschreibungspflicht entzogen, wenn mit der Ausübung der automatischen Verlängerungsklausel keine Anpassungsvereinbarungen verbunden werden.
Ist beabsichtigt, Leistungen in Form einer **Rahmenvertrages** (vgl. S. 40) zu vergeben, in dem die Bedingungen für Einzelaufträge festgelegt werden, die im Laufe eines bestimmten Zeitraums vergeben werden sollen, bedarf es im Folgenden keiner Ausschreibung der Einzelaufträge, wenn diese in dem Rahmenvertrag bereits hinreichend konkretisiert sind. Bei einem Rahmenvertrag handelt es sich um eine Vereinbarungen mit einem oder mehreren Unternehmen, in der die Bedingungen für Einzelaufträge festgelegt werden, die im Laufe eines bestimmten Zeitraums vergeben werden sollen, insbesondere über den in Aussicht genommenen Preis und gegebenenfalls die in Aussicht genommene Menge (vgl. § 3 Abs. 8 Satz 2 VgV). Rahmenverträge über IT-Leistungen bedürfen daher bereits bei der Ausschreibung einer möglichst konkreten Beschreibung des Leistungsgegenstandes.

Was muss Inhalt der Vergabeunterlagen sein?

Die **Vergabeunterlagen** bestehen aus der **Aufforderung zur Angebotsabgabe** und den Verdingungsunterlagen (§ 9 Nr.1 VOL/A). Verdingungsunterlagen umfassen die Gesamtheit der Aufzeichnungen, in denen die technische Beschreibung der zu vergebenden Leistungen und die rechtlichen und wirtschaftlichen Vertragsbedingungen festgelegt sind. Inhaltlich ist strikt zwischen der Festlegung von Eignungs-, Auftragskriterien und der Beschreibung der Leistung zu trennen. Nur bei der Leistungsbeschreibung gibt es Besonderheiten bei IT-Verträgen.

Die **Beschreibung der Leistung** muss eindeutig und erschöpfend sein. Es sind die näheren Vorgaben gemäß § 8 VOL/A zu berücksichtigen. Bei Abschluss von IT-Verträgen sollte in der Regel bereits hier eine Beschreibung der erforderlichen Leistungen in einem sog. **Pflichtenheft** erfolgen. Inhaltlich enthält ein Pflichtenheft insbesondere eine allgemeine Zielbeschreibung, die Beschreibung des Ist-Zustandes, den Funktionsumfang, Leistungsnachweise, Leistungsumfang sowie Test und Abnahmebedingungen.

Verträge über die Beschaffung von IT-Leistungen sind grundsätzlich auf **Grundlage der Allgemeinen Vertragsbedingungen** für die Ausführung von Leistungen (VOL/B) abzuschließen. Nach § 9 Nr. 2 VOL/A ist bereits in den Verdingungsunterlagen vorzuschreiben, dass diese Bedingungen Bestandteil der Vertrages werden. Das gilt ebenso für zusätzliche, ergänzende und besondere Vertragsbedingungen.

4.1.2 Welche Regelungsaspekte sollten umfasst werden?

Welche standardisierten Vertragsbedingungen sind grundsätzlich zu beachten?

Bei Abschluss von IT-Verträgen sind grundsätzlich die **Allgemeinen Vertragsbedingungen** (VOL/B) zu beachten. Daneben bestehen für viele Arten von IT-Leistungen **spezielle standardisierte Ergänzende Vertragsbedingungen für den IT-Bereich** (BVB-EDV/EVB-IT).

Die **VOL/B** können eine individuelle, auf eine bestimmte Dienstleistung abgestimmte Gestaltung eines Vertrages nicht ersetzen. Darüber hinaus kann von den Allgemeinen Vertragsbedingungen (VOL/B) nach § 9 Nr. 3 Abs. 2 Satz 3 VOL/A insbesondere abgewichen werden, wenn:

- diese auf die Fälle beschränkt werden, für die besondere Vereinbarungen in den VOL/B ausdrücklich vorgeschrieben sind;
- die Abweichungen nicht weiter gehen als es die Eigenart der Leistung und ihre Ausführung erfordern.

Die älteren BVB-EDV werden derzeit sukzessive durch abgestimmte neue **Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT)** abgelöst. Für die Bereiche Kauf, Dienstleistung (Schulungs-, Beratungs- oder sonstige Unterstützungsleistungen), Überlassung von Standardsoftware und Instandhaltung von EDV-Anlagen und Geräten wurden bereits neue EVB-IT eingeführt. Insbesondere für komplexe Verträge (z.B. Individual-Systeme von Software oder Hardware auf Basis eines Phasenkonzepts, Systemverträge und Systemservices, Daten- und Serverbetrieb) bestehen zwar bisher keine EVB-IT, sind jedoch bereits geplant.

Der Kooperationsausschuss Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA/ADV) hat seinen Mitgliedern empfohlen, die EVB-IT einzuführen. Bund und Länder haben teilweise die Verwaltungsvorschriften zur BHO und LHO entsprechend angepasst oder dürften dies noch tun. Die Gemeinden entscheiden jeweils selbst, ob sie die EVB-IT für verbindlich erklären. Auch wenn keine Verbindlichkeit festgelegt ist, können sie zumindest eine Orientierung für die zu beachtenden Vertragsinhalte und Regelungsaspekte bilden.

Selbst bei einer Bindung kann auf **die Anwendbarkeit der EVB-IT** grundsätzlich **verzichtet** werden, wenn:

für die Leistungen aus besonderen Gründen (z.B. besondere Erfahrungen, Zuverlässigkeit, bestimmte Ausführungsarten, bestehende Schutzrechte) nur ein Unternehmen in Betracht kommt und dieses Unternehmen nicht bereit ist, die EVB-IT als Vertragsunterlage anzuerkennen;

infolge der Anwendung der EVB-IT die Beschaffung insgesamt unwirtschaftlich wäre.

Die EVB-IT bestehen jeweils aus einem Vertragsformular und aus Allgemeinen Geschäftsbedingungen. Die Dokumente können abgerufen werden unter: www.kbst.bund.de

Die EVB-IT sind lediglich für Standardfälle geschaffen. Komplexe oder abweichende Aufgaben sollen die EVB-IT nicht abschließend lösen. Im Einzelfall können die Vertragsbedingungen daher durch **besondere Vertragsbedingungen** ergänzt werden.

Welche speziellen zusätzlichen Regelungsaspekte sollten umfasst werden?

Wegen der Unterschiedlichkeit der möglichen IT-Dienstleistungsverträge kommt der **individuellen Vertragsgestaltung** auch bei Einbeziehung der Vertragsbedingungen eine besondere Bedeutung zu. Neben den allgemeinen bei Verträgen zu berücksichtigenden Inhalten (z.B.: Haftung, Gewährleistung, Kündigung u.s.w.), sollten insbesondere folgende Punkte umfasst werden:

- Um den Interessen der Verwaltung gerecht zu werden, kommt es insbesondere auf eine auf den individuellen Bedarf zugeschnittene **detaillierte und eindeutige Beschreibung des Leistungsgegenstandes**, ggf. durch ein Pflichtenheft an.
- Soweit sensible Bereiche und Daten betroffen sind, sollten genaue Sicherheitsstandards vorgegeben und die Einhaltung von speziellen **Datenschutzvorgaben** sichergestellt sowie **Geheimhaltungsverpflichtungen** getroffen werden. Entsprechend sollte festgelegt werden, unter welchen Voraussetzungen der Auftragnehmer zur Erfüllung seiner Pflichten **Dritte einschalten** darf.
- Daneben sollte vertraglich geregelt werden, wie die erbrachten Leistungen zu messen und zu dokumentieren sind.
- Soweit aus der Zusammenarbeit schutzrechtsfähige Erfindungen hervorgehen, sollte geregelt werden, inwieweit dem Auftragnehmer **Nutzungsrechte** zustehen.

Was ist bei Outsourcing-Verträgen zusätzlich zu beachten?

Bei der umfassenden Auslagerung oder Ausgliederung von Datenverarbeitungsleistungen (Outsourcing) ist aufgrund der intensiven und langfristigen Bindung eine besondere Sorgfalt auf die Vertragsgestaltung zu legen. Als Vertragsform kommt insbesondere ein Rahmenvertrag mit mehreren Anlagen in Betracht. Die zu erbringenden Leistungen werden in den leicht anzupassenden Anlagen (z.B. in Form eines sog. Pflichtenheftes) genauer definiert. Zu den bei Rahmenvereinbarungen zu beachtenden vergaberechtlichen Vorgaben vgl. S. 38. Über die bei IT-Verträgen insbesondere zu beachtenden Vertragsinhalte (vgl. S. 39 und S. 40) hinaus, gibt es bei Outsourcing-Vorhaben weitere spezifische Punkte, die insbesondere zu berücksichtigen sind:

- Bei langfristigen Vorhaben kommt für das Projektcontrolling und die Projektkoordination die Einrichtung eines **Lenkungs- oder Koordinierungsausschusses** in Betracht;
- soweit umfangreiche technische Dienstleistungen (z.B. Server- und Datenbankbetrieb) outgesourct werden, hat die Gewährleistung eines **dauerhaften störungsfreien Betriebs** hohe Priorität. Sinnvoll ist, genaue Regelungen zum Verhalten bei und zur Behebung von Störfällen einzubinden;
- für die Beendigung der Partnerschaft sollte eine Klausel aufgenommen werden, in der die **nachvertraglichen Pflichten** festgelegt werden. Dazu gehört insbesondere die Regelung, welche Unterlagen/technischen Entwicklungen auf den Outsourcing-Geber übertragen werden. Insbesondere dürfen im Falle der Auftragsdatenverarbeitung beim Outsourcing-Nehmer nach den Datenschutzgesetzen keine personenbezogenen Daten verbleiben;
- zu weiteren datenschutzrechtlichen Vorgaben vgl. S. 35.

4.2 Was ist beim Eingehen von Entwicklungspartnerschaften zu bedenken?

Für die Einbindung privaten Know Hows kommt das Eingehen einer (Produkt-) Entwicklungspartnerschaft in Betracht. Charakteristisch für diese Art von Partnerschaft ist der Zusammenschluss der öffentlichen Hand mit einem privaten Partner, der ohne oder gegen geringe Gegenleistung für den Bereich des E-Government IT-Lösungen entwickelt.

4.2.1 Was ist bei der Auswahl der privaten Partner zu beachten?

Grundsätzlich ist die Entwicklungspartnerschaft von einem **Entwicklungsauftrag** abzugrenzen. Während bei der Entwicklungspartnerschaft keine Vergütung des Auftragnehmers erfolgt, werden bei einem Entwicklungsauftrag gewisse Entwicklungsleistungen vollständig durch den Auftraggeber vergütet, so dass das Vergaberecht grundsätzlich anzuwenden ist (vgl. grundsätzlich zur Anwendbarkeit von Vergaberecht S. 25). Die **vergaberechtliche Einordnung**

von **Entwicklungspartnerschaften** ist noch **nicht abschließend geklärt**. Auch hier kommt es auf eine Betrachtung des Einzelfalles an.
Für Aufträge oberhalb des Schwellenwertes bestimmt § 100 Abs. 2 n) GWB, dass Forschungs- und Entwicklungsleistungen nicht dem Vergaberecht unterfallen, es sei denn, ihre Ergebnisse werden ausschließlich Eigentum des Auftraggebers für seinen Gebrauch bei der Ausübung seiner eigenen Tätigkeit und die Dienstleistung wird vollständig durch den Auftraggeber vergütet. Eine ähnliche Regelung enthält auch § 2 Abs. 3 b) VOF für Leistungen, die als freiberufliche Leistungen einzuordnen sind. Teilweise wird aber im Hinblick auf § 100 Abs. 2 n) GWB eine einschränkende Auslegung verlangt, die dahin zielt, dass entsprechend der europarechtlichen Vorgaben nur gemeinnützige Forschungs- und Entwicklungsleistungen von den Vergaberegeln freigestellt werden sollen.
In jedem Fall ist bei einer Entwicklungspartnerschaft grundsätzlich die **Anwendbarkeit des Verhandlungsverfahrens** zulässig, wenn es sich um die Lieferung von Waren handelt, die nur zum Zwecke von Forschungen und Entwicklungen hergestellt werden (vgl. § 3 a Nr. 2 b) VOL/A). Regelmäßig kann die Leistung nach Art und Umfang vor der Vergabe auch nicht so eindeutig und erschöpfend beschrieben werden, dass hinreichend vergleichbare Angebote erwartet werden können (§ 3 Nr. 4 h) VOL/A).

4.2.2 Welche Regelungsaspekte sollten umfasst werden?

Regelmäßig ist im Rahmen der Entwicklungspartnerschaft eine eindeutige und umfassende Beschreibung konkreter Leistungsinhalte nicht möglich. Allerdings kann durch gemeinsame **Zielvorgaben** das Ergebnis der angestrebten Leistung näher präzisiert werden.
Die konkreten Zielvorgaben sind dabei abhängig von dem Bereich, in dem die Entwicklung stattfinden soll. Aus Sicht der Verwaltung sollten beim Aufsetzen der Entwicklungspartnerschaft insbesondere folgende Regelungsaspekte umfasst sein:

- Möglichst konkrete **Festlegung der Zielvorgaben**;
- Einhaltung **datenschutzrechtlicher Vorgaben** (vgl. S. 35);
- Festlegung des Investitionsvolumens der privaten Partner um **Planungssicherheit** zu erreichen;
- **Einbindung von Verwaltungsmitarbeitern** um nachhaltige Lerneffekte für die Verwaltung und ein Controlling des Projektes sicherzustellen;
- **Vertraulichkeits-/Geheimhaltungsverpflichtung**;
- Festlegung von **Meilensteinen** und einer **Frist für das Projektende** damit sich die Verwaltung bei Scheitern des Projekts zeitnah anders orientieren kann;
- **Sicherstellung von Nutzungsrechten** der Verwaltung an den entwickelten Produkten.

Weiterführende Literatur und Rechtsprechung:
Zum Application Service Providing: *Daum*, Die Rolle öffentlicher Unternehmen im Application Service Providing, ZögU 2002, S. 263ff. Zu den vergaberechtlichen Vorgaben: *Kulartz,/Steding*, IT-Leistungen, Fehlerfreie Ausschreibungen und rechtssichere Vertragsinhalte, 1. Aufl. 2002; *Hertwig*, Praxis der öffentlichen Auftragsvergabe: VOB/VOL/VOF, 2 Aufl. 2001; *Daub/Meierrose*, Kommentar zur VOL/A, 5. Aufl. 2000. Zur Anwendbarkeit von Vergaberecht bei langfristigen Verträgen: 2. Vergabekammer des Bundeskartellamts, Beschluss vom 26.5.2000, VK 2 -8/00, abzurufen unter www.bundeskartellamt.de/archiv.html. Zu den Ergänzenden Vertragsbedingungen BVB/EVBiT: *Kulartz/Steding*, IT-Leistungen, Fehlerfreie Ausschreibungen und rechtssichere Vertragsinhalte, 1. Aufl. 2002; *Leitzen/Intveen*, IT-Beschaffungsverträge der öffentlichen Hand, Die neuen EVB-IT als BVB-Nachfolger, CR 2001, S. 493ff.. Allgemein zum Outsourcing: *Lütcke/Bähr*, Outsourcing-Verträge und Service Level Agreements in der IT-Branche – Gestaltungsvarianten für die Praxis, K&R 2001, S. 82ff.; *Köhler-Frost* (Hrsg.), Outsourcing - Eine strategische Allianz besonderen Typs, 4. Aufl. 2000. Zum Inhalt eines Pflichtenhefts bei IT-Verträgen: *OLG Düsseldorf*, CR 1993, S. 361ff.
Praxisbeispiele:
Zu Kooperationsbeispielen zur Einbindung von IT-Know How: *Stapel-Schulz/Eifert* (Hrsg.), Organisations- und Kooperationstypen kommunaler Internetauftritte, Arbeitspapier 6/2002 aus der Begleitforschung zum Städtewettbewerb MEDIA@Komm, abzurufen unter www.mediakomm.net, S. 16ff. Für Entwicklungspartnerschaften: Kooperation zwischen der Stadt Mannheim und der SAP AG zur Entwicklung von 6 Bürgerdiensten, vgl. www.mannheim.de; Kooperation in Hagen zwischen HABIT und der Interactive World Media Systems GmbH, vgl. http://vrhagen.stadt-hagen.de.

5. Allgemeine Vorgaben für alle Angebotstypen

Grundlegende Anbieterpflichten gelten für alle Online-Dienste der Verwaltung unabhängig davon, ob sie Informations-, Kommunikations- oder Transaktionsangebote sind. Sie ergeben sich vor allem aus der medienrechtlichen Einordnung als Medien- oder Teledienst.

5.1 Wie sind die einzelnen Angebote medienrechtlich einzuordnen?

Rechtliche Regelungen für private wie öffentliche Anbieter von Online-Diensten enthalten insbesondere der **Mediendienstestaatsvertrag** (MDStV), das **Teledienstegesetz** (TDG) und für die Verwendung von Nutzerdaten das **Teledienstedatenschutzgesetz** (TDDSG). Für Telekommunikationsdienste gilt das **Telekommunikationsgesetz** (TKG). Zur strittigen Einordnung von E-Mail-Diensten vgl. unten S. 62.

Während der MDStV für Mediendienste die einschlägige Regelung darstellt, richtet sich das TDG an Anbieter von Telediensten. Die Regelungen beider Gesetze gelten auch für amtliche Behördenangebote. Beide Gesetze enthalten im jeweiligen § 2 eine Definition ihres Geltungsbereiches. Als Grundformel ergibt sich hieraus, dass sich der Geltungsbereich des MDStV auf das Angebot und die Nutzung von an **die Allgemeinheit** (also eine unbestimmte Zahl möglicher Nutzer) **gerichteten Informations- und Kommunikationsdiensten** erstreckt, während das TDG für alle elektronischen Informations- und Kommunikationsdienste gilt, die für **eine individuelle Nutzung (Individualkommunikation)** bestimmt sind. Beide Gesetze enthalten darüber hinaus eine nicht abschließende Aufzählung vom jeweiligen Geltungsbereich erfasster Dienste. Mediendienste sind hiernach gem. § 2 Abs. 2 MDStV z.B. Angebote des Teleshopping, Textdienste und Abrufdienste (soweit bei letzterem nicht der individuelle Leistungsaustausch im Vordergrund steht). Teledienste sind z.B. gem. § 2 Abs. 2 TDG das Angebot des Telebanking oder der individuelle Datenaustausch über Datendienste (z.B. Verkehrs-, Wetter-, Umwelt- und Börsendienste). Bei der Möglichkeit des interaktiven Zugriffs und einer unmittelbaren Bestellmöglichkeit zählt auch das Angebot von Waren und Dienstleistungen zum Teledienst, denn auch hier steht die individuelle Kommunikation im Vordergrund.

In der Praxis kann sich eine Zuordnung einzelner Dienste als problematisch erweisen, da die rechtlichen Bestimmungen keiner einheitlichen Systematik folgen. Hier hilft es, sich zunächst an den dargestellten Regelbeispielen der Gesetze zu orientieren. Helfen diese nicht weiter, so kann auch auf die Inhalte der Dienste abgestellt werden. Ist überhaupt keine klare Einordnung möglich, so sollte im Einzelfall das Angebot so aufgebaut sein, dass den Regelungen beider Gesetze entsprochen wird (soweit dies möglich ist).

5.2 Bestehen abweichende Anforderungen an Medien- und Teledienste?

Die rechtlichen Auswirkungen einer unterschiedlichen Einordnung der Dienste in der Praxis sind eher gering. Denn zahlreiche Regelungen weisen inhaltlich eine große Übereinstimmung auf:

- Sowohl Mediendienste als auch Teledienste sind **zulassungs- und anmeldefrei** (§ 4 MDStV / § 5 TDG).
- Auch gilt für Tele- und Mediendienste gleichermaßen das Gebot der Datenvermeidung. § 4 Abs. 6 TDDSG als auch § 13 Abs. 1 MDStV fordern daher das **Angebot pseudonymer Nutzungs- und Bezahlverfahren**.
- Sowohl bei dem Angebot eines Tele- als auch eines Mediendienstes ist der **Impressumspflicht** Rechnung zu tragen (§ 6 TDG / § 10 MDStV). Siehe zur allgemeinen Kennzeichnungspflicht für Diensteanbieter unten S. 43.
- Ist eine Online-Registrierung vor Nutzung eines Diensteangebots notwendig und werden hierbei personenbezogene Daten erhoben, so legt sowohl § 18 Abs. 1 MDStV als auch § 4 Abs. 1 TDDSG fest, dass der Nutzer vor einer Erhebung über Umfang, Ort und Zweck der Erhebung zu **unterrichten** ist. Der Diensteanbieter hat auf das **Recht zum Widerruf** erteilter Einwilligungen hinzuweisen (vgl. auch S. 50).
- Eine **gültige elektronische Einwilligung zur Datenerhebung und Datenverarbeitung** ist für Tele- wie für Mediendienste auch ohne qualifizierte elektronische Signatur möglich (§ 4 Abs. 2 TDDSG / § 18 Abs. 2 MDStV, vgl. hierzu S. 47).
- Gleichlautende Regelungen enthalten der MDStV und das TDDSG auch für die Erstellung von Nutzerprofilen. Ein Diensteanbieter darf nur für Zwecke der Marktforschung, der bedarfsgerechten Gestaltung des Dienstes oder für Zwecke der Werbung **Nutzerprofile unter Verwendung von Pseudonymen** erstellen (§ 6 Abs. 3 TDDSG / § 19 Abs. 4 MDStV).
- Sowohl für Mediendienste (§§ 6ff. MDStV) als auch für Teledienste (§§ 8ff. TDG) bestehen Vorschriften der

Haftungsprivilegierung für Inhalte Dritter (siehe zum Umfang der Haftung S. 43 und 57).

Weiterführende Literatur:
Zur grundsätzlichen Einordnung der Dienste: Hamburger Datenschutzbeauftragter Orientierungshilfe Tele- und Mediendienste, Stand 1. Juli 2002, abrufbar unter www.hamburg.datenschutz.de; *Schaar,* Datenschutz im Internet, 2002, S. 78ff.; *Roßnagel/Banzhaf/ Grimm*, Datenschutz im E-Commerce, 2003, S. 124ff. Ein Wegweiser zu den Informations- und Kommunikationsdienste-Gesetzen und weiteren Gesetzen für die Informationsgesellschaft findet sich auf einer Webseite des BMWA unter www.iukdg.de.

5.3 Welche allgemeinen Haftungsgrundsätze sind zu beachten?

Für Medien- und Teledienste existieren identische **spezielle Haftungsregelungen** zur Verantwortlichkeit von Betreibern eines Internetportals, die für alle Rechtsgebiete und Anwendungsbereiche gültig sind und die elektronische Kommunikation in ihrer Entwicklung begünstigen sollen.
Für **eigene Inhalte** haftet der Betreiber grundsätzlich nach den allgemeinen Gesetzen (§ 8 TDG/§ 6 MDStV). Für **fremde Inhalte** haftet der Betreiber dagegen grundsätzlich erst ab Kenntnis der Rechtswidrigkeit der Inhalte und soweit er nicht unverzüglich tätig geworden ist, um die Informationen zu entfernen oder den Zugang zu ihnen zu sperren (§ 11 TDG/ § 9 MDSt). Wird lediglich der Zugang zur Nutzung von Informationen vermittelt, besteht ebenfalls grundsätzlich keine Haftung (§ 9 TDG/§ 7 MDStV). Von besonderer Relevanz sind insbesondere:
die allgemeinen Vorgaben für die Haftung für Informationsangebote (vgl. S. 57);
die Haftung für rechtswidrige Inhalte in Hyperlinks (vgl. S. 57).

Weiterführende Literatur:
Engels, Zivilrechtliche Haftung für Inhalte im World Wide Web, AfP 2000, S. 524ff.; *Hoeren*, Internetrecht, Stand: Oktober 2002, S. 341ff., abzurufen unter: www.uni-muenster.de/Jura.itm/hoeren/material/skript.pdf.

5.4 Welche allgemeinen Kennzeichenpflichten sind zu beachten?

Wird ein Angebot als Mediendienst eingeordnet, so besteht gem. § 10 Abs. 1 MDStV die Pflicht für jeden Anbieter, Namen und Anschrift anzugeben **(einfache Anbieterkennzeichnung).** Bei Personenvereinigungen und -gruppen, unter welche auch juristische Personen zu fassen sind, ist weiter auch Name und Anschrift der Person zu nennen, der Außenvertretungsbefugnis zukommt.
Werden **geschäftsmäßige Mediendienste** angeboten, so kommt gem. § 10 Abs. 2 TDG die Pflicht hinzu, Information über Name und Anschrift, unter der sie niedergelassen sind einzustellen, sowie Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen. Des Weiteren muss die Adresse der elektronischen Post bereitgehalten werden. Bei juristischen Personen müssen zusätzlich Angaben über den Vertretungsberechtigten erfolgen. Ein geschäftsmäßiger Mediendienst soll bereits dann vorliegen, wenn das Online-Angebot auf einer gewissen Nachhaltigkeit (Dauer) beruht. Dies wird für Online-Angebote der Verwaltung fast immer der Fall sein. Eine zusätzliche Gewinnerzielungsabsicht ist nicht notwendig.
Ist darüber hinaus das Angebot des Mediendienstes **journalistisch-redaktionell** gestaltet und weist es periodische Bezüge auf, muss gem. § 10 Abs. 3 MDStV zusätzlich ein Verantwortlicher mit Anschrift genannt werden **(qualifizierte Anbieterpflicht**). Werden durch die Verwaltung **mit kommerzieller Kommunikation vergleichbare Dienste** angeboten, sollte letztlich auch den erhöhten Hinweispflichten aus § 10 Abs. 4 MDStV entsprochen werden.
Gleichlautend sind die Anforderungen, wenn ein Teledienst durch die Verwaltung angeboten wird. Die allgemeinen Informationspflichten richten sich nach § 6 TDG, die besonderen Informationspflichten nach § 7 TDG.
Zumindest eine einfache Kennzeichnungspflicht (Name/Anschrift) wird für Internet-Angebote der Kommunen und Städte daher immer vorliegen. Die Informationen sind durch den Diensteanbieter **leicht erkennbar, unmittelbar erreichbar** und **ständig verfügbar** zu halten. Die Darstellung des Impressums einer Website unter dem Begriff „Backstage", der erst erkennbar wird, wenn nach rechts gescrollt wird, erfüllte nach Ansicht des LG Hamburg diese Anforderungen z.B. nicht.

Weiterführende Literatur und Rechtsprechung:
Zur Anbieterkennzeichnung nach § 6 Nr. 2 TDG a.*F OLG München*, Urt. v. 26.07.2001, JurPC Web-Dok. 43/2002; *Brönneke*, in: Roßnagel (Hrsg.), Recht der Multimediadienste, Kommentierung zu § 6 TDG und Ukrow, ebenda, Kommentierung ui § 6 MDStV (alt) und § 10 MDStV (neu) i.E. Zur Anbieterkennzeichnung nach Neufassung des TDG: *Weber*, Der Adressatenkreis der Verpflichtung zur Anbieterkennzeichnung im Internet nach der Neufassung des Teledienstegesetzes, JurPC Web-Dok. 76/2002; Hamburger Datenschutzbeauftragte, Orientierungshilfe Tele- und Mediendienste, Stand 1. Juli 2002, abrufbar unter www.hamburg.datenschutz.de. Zur Form der Darstellung: *LG Hamburg*, Urt. v. 26.08.2002, JurPC Web-Dok. 370/2002.

5.5 Wie sind Datenschutzhinweise durch die Verwaltung auszugestalten?

Werden personenbezogene Daten verarbeitet, ist eine datenschutzrechtliche Unterrichtung notwendig. Die Datenschutzbeauftragten des Bundes und der Länder führen hierzu aus: „Nur wenn die Bürgerinnen und Bürger wissen, wie die Datenverarbeitungsvorgänge ablaufen, haben sie auch die Möglichkeit, ihre Rechte wahrzunehmen. Für viele Nutzer wird allerdings nicht ohne weiteres erkennbar sein, an welchen Stellen sie bei Nutzung elektronisch zur Verfügung gestellter Informationen Spuren hinterlassen bzw. inwieweit personenbezogene Nutzerdaten weiterverarbeitet werden. Das TDDSG und der MDStV verpflichten die Diensteanbieter für den Fall der automatisierten Weiterverarbeitung personenbezogener Daten, die Nutzer zu Beginn des Verfahrens zu unterrichten. Nur die Vorabinformation versetzt die Nutzer in die Lage darüber zu entscheiden, ob sie das Nutzungsverhältnis fortsetzen oder abbrechen möchten." Hieraus ergeben sich für die Gestaltung von Datenschutzhinweisen folgende Empfehlungen der Bundes- und Landesdatenschutzbeauftragten:

- „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 sollten leicht verständlich formuliert sein. Zur Gewährleistung der Transparenz gehört insbesondere die Information darüber, wer für die Gestaltung des Angebots verantwortlich zeichnet.

Öffentliche Stelle: <Name>
Verantwortlich: <Name> <Adresse>
Telefon: <Nr.>
Telefax: <Nr.>
E-Mail: <E-Mail Adresse>

- Bei Links und E-Mail-Adressen sollte ein Hinweis auf die Risiken bzw. den Haftungsausschluss aufgenommen werden. Dies kann auch durch eine allgemeine Information in den Datenschutzhinweisen erfolgen. Es ist auch möglich, beim „Überstreichen" eines Links oder einer E-Mail-Adresse den Hinweis automatisch aufzublenden. Bei Koppelung des Verwaltungsauftritts mit privaten Sponsoren muss für die Nutzer deutlich erkennbar sein, wer für welches Angebot die Verantwortung trägt.

- 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. Wenn Daten in Log-Dateien gespeichert werden, könnte eine Information folgendermaßen aussehen:

Textbeispiel:
Mit Ihrem Zugriff auf diese Seite werden die um die letzten 3 Ziffern verkürzte IP-Adresse Ihres Rechners und weitere Angaben (Datum, Uhrzeit, betrachtete Seite) auf unserem Server für Zwecke der Datensicherheit für zwei Monate gespeichert. Die Daten werden außerdem für statistische Zwecke ausgewertet. Durch die Verkürzung der IP-Adresse ist der Bezug der gespeicherten Daten auf Ihre Person ausgeschlossen. Wir verwenden keine Cookies, Java-Applets oder Active-X-Controls. Sollten Sie noch Fragen zum Datenschutz haben, wenden Sie sich bitte an: Name: E-Mail-Adresse. Telefon:

- Sollten Cookies verwendet werden, so muss die Information auch einen Hinweis über deren Auswirkungen enthalten. Mit der Verwendung aktiver Elemente wie Active-X, Java, JavaScript sollten öffentliche Verwaltungen restriktiv umgehen. Die wesentlichen Informationen und Serviceleistungen sollte jeder Bürger ohne Eingehen der mit diesen Elementen verbundenen Risiken nutzen können. Sollte jedoch eine Verwaltung trotzdem nicht völlig auf die Nutzung dieser Elemente verzichten wollen, so hat sie den Nutzer auch hierüber zu informieren und ihn auf die Risiken hinzuweisen.
- Bei elektronischer Antragstellung ist der Antragsteller darüber zu informieren, wie das Gesamtverfahren abgewickelt wird. Sollten im Rahmen von E-Government-Anwendungen mobile Speichermedien zum Einsatz kommen, so muss für den Betroffenen erkennbar sein, welche Daten und Programme mit welchen Funktionen auf seiner Karte gespeichert sind. Insbesondere muss er erkennen können, wer welche Daten und Programme mit welchen Funktionen auf seiner Karte speichert (Schreibberechtigung) und wer welche Daten nutzen kann (Leseberechtigung). Zudem muss die Möglichkeit gegeben sein, den Inhalt der gespeicherten Informationen zur Kenntnis zu nehmen. Ferner ist er darüber zu unterrichten, welche Maßnahmen bei Verlust oder Zerstörung des Mediums zu treffen sind

und welche Verfahren bei der verantwortlichen Stelle im Hintergrund ablaufen.

- Um für die Nutzer ein hohes Maß an Transparenz zu gewährleisten, sollten die Datenschutzerklärungen bei E-Government-Anwendungen den P3P-Standard (www.w3c.com/p3p) einhalten."

5.6 Was ist für die Einbeziehung von Benutzungsbedingungen, Haftungsausschlüssen und Datenschutzhinweisen zu beachten?

Sollen Benutzungsbedingungen (inkl. Haftungsausschlüsse und Datenschutzhinweise) wirksam in die Nutzung des Internetangebots der Verwaltung einbezogen werden, so müssen bestimmte Vorgaben beachtet werden. Zunächst sind **Benutzerbedingungen gut sichtbar** zu gestalten und in das Webangebot zu integrieren. Dies kann auf unterschiedlichen Wegen erfolgen. Weit verbreitet ist die Lösung, weiterführende Links, z.B. zum Forum, zugleich mit dem Hinweis zu verbinden, dass die aufgestellten Bedingungen für eine Nutzung des Forums zur Kenntnis genommen und akzeptiert wurden. Eine **konkludente Akzeptanz der Benutzungsbedingungen** wird dann durch Aufruf des Web-Angebots abgegeben. Ähnlich der Einbeziehung von allgemeinen Geschäftsbedingungen (AGB) muss hierbei allerdings sichergestellt sein, dass für den User zumindest die **Möglichkeit zur Kenntnisnahme** über Inhalt und Umfang der Nutzungsbedingungen in zumutbarer Weise bestand. Nur dann kann sich der Anbieter eines Forums auch auf diese berufen. Ob der User tatsächlich die Nutzungsbedingungen aufgerufen und sich inhaltlich mit ihnen auseinandergesetzt hat, soll dagegen nach h.M. nicht entscheidend sein. Gleichwohl kann das Webangebot auch so gestaltet werden, dass der User tatsächlich die Nutzungsbedingungen zur Kenntnis genommen haben muss. Dies wird vor allem erreicht, wenn die Benutzerbedingungen nicht bloß hinterlegt und über einen Link erreichbar gemacht werden, sondern ihr Aufruf durch die Gestaltung des Web-Angebots notwendiger Zwischenschritt zur Erreichung des weiteren Online-Angebots ist (Gate-Funktion).

Für **die Einbeziehung einer Einwilligung in die Verarbeitung personenbezogener Daten** ist zu beachten, dass hier die bloße Möglichkeit zur Abgabe einer Willenserklärung (Einwilligung) nicht ausreicht, vielmehr eine singuläre, inhaltlich begrenzte Willenserklärung zu erfolgen hat. Schweigen und die gleichzeitige Annahme eines Web-Angebots kann daher hier gerade nicht als konkludente Einwilligung angesehen werden (zur Einwilligung generell und zur Möglichkeit der elektronischen Einwilligung siehe unten S. 47).

Weiterführende Rechtsprechung:
Zur elektronischen Vereinbarung von AGB: *OLG Hamburg*, Urt. v. 13.06.2002, JurPC Web-Dok. 288/2002.

5.7 Welche allgemeinen Datenschutzgrundsätze sind bei einer Internettätigkeit der Verwaltung zu beachten?

Auch bei einer Internettätigkeit der Verwaltung gelten die allgemeinen Datenschutzgrundsätze, wie sie das Bundesverfassungsgericht (BVerfG) im sog. „Volkszählungsurteil" (*BVerfGE* 65, 1 ff.) als Anforderungen an einen verfassungsgemäßen Datenschutz formuliert hat. Der einzelne Bürger ist hiernach über sein allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 des GG vor einer übermäßigen Erhebung, Speicherung, Weitergabe und Verwendung seiner persönlichen Daten geschützt **(Recht auf informationelle Selbstbestimmung).** Zur Konkretisierung dieses Schutzerfordernisses wurden allgemeine Datenschutzgrundsätze formuliert. Sie gelten weitgehend für öffentliche wie für nicht-öffentliche Stellen und finden daher sowohl bei direkter Verwaltungstätigkeit über das Internet, aber auch bei einer Realisierung von Online-Projekten mit oder ganz durch Private Anwendung.

5.7.1 Welche gesetzlichen Grundlagen sind für ein datenschutzgerechtes E-Government relevant?

Hierzu führen die Datenschutzbeauftragten des Bundes und der Länder aus: "Beim E-Government werden die Möglichkeiten der elektronischen Kommunikation über das Internet genutzt. Dabei können Daten an einem Ort erhoben, an einem anderen Ort gespeichert und an einem dritten Ort genutzt werden. Hierfür gibt es keine verbindlichen internationalen Datenschutz-Standards, gleichwohl werden von den meisten Beteiligten im Internet einige Grundregeln freiwillig beachtet. In der Bundesrepublik Deutschland sind hierfür komplexe rechtliche Rahmenbedingungen geschaffen worden, die insbesondere den Umgang mit den bei der elektronischen Kommunikation anfallenden Bestands-,

Verbindungs-, Nutzungs- und Inhaltsdaten regeln. Bei Einrichtung und Betrieb von Internet-Diensten sind im Einzelnen folgende Datenschutz-Vorschriften zu beachten:

- für die erste Ebene: das Telekommunikationsgesetz (TKG) und die Telekommunikationsdatenschutzverordnung (TDSV) (Anm. der Autoren: Die erste Ebene betrifft insbesondere sog. **Verbindungsdaten**, die bei der Erbringung von Telekommunikationsleistungen anfallen);
- für die zweite Ebene: das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) sowie der Mediendienstestaatsvertrag (MDStV), (Anm. der Autoren: Die zweite Ebene betrifft die sog. **Nutzungsdaten**, also solche Daten, die bei eine Inanspruchnahme der Dienste anfallen);
- für die dritte Ebene: die allgemeinen Datenschutzvorschriften im Bundesdatenschutzgesetz, in den Datenschutzgesetzen der Länder sowie in anderen bereichsspezifischen Gesetzen, (Anm. der Autoren: Die dritte Ebene betrifft die sog. **Inhaltsdaten**, also solche Daten, die unabhängig vom jeweiligen Dienst bestehen und nur über diesen transportiert werden).

Dabei gilt auf der zweiten Ebene für Anwendungen, die auf eine individuelle Nutzung ausgerichtet sind, das Teledienstegesetz und das Teledienstdatenschutzgesetz. Darunter fallen z.B. die elektronische Anforderung von Antragsunterlagen (Wahlunterlagen, Bauanträge), elektronische Bestellverfahren (Müllsäcke, Sperrmüllabfuhr), Gästebücher, Telearbeit etc. Elektronische Informations- und Kommunikationsdienste, die sich an die Allgemeinheit richten, fallen dagegen unter das Medienrecht. Dazu gehören insbesondere Informationsangebote und Abrufdienste mit redaktioneller Gestaltung, wie z.B. der Pressespiegel. Die drei Ebenen umfassen die folgenden Regelungsschichten:

Abbildung 4: Regelungsebenen im Datenschutz

Ebene	Wesentliche Forderungen	Beispiel
Ebene 1: Transportebene **Rechtsgrundlage:** Telekommunikationsrecht (TKG, TDSV)	Fernmeldegeheimnis; Technische Schutzmaßnahmen; Umgang mit Bestands-, Verbindungs- und Abrechungsdaten.	Netzbetrieb; Zugang zum Internet
Ebene 2: Transportbehälterebene **Rechtsgrundlage:** "Online-Recht" (Teledienstdatenschutzgesetz, Mediendienste-Staatsvertrag)	Informations- und Kennzeichnungspflichten; Verantwortlichkeiten für die angebotenen Informationen; Umgang mit Bestands-, vorgangsbezogenen Nutzungs- und Abrechnungsdaten; Widerspruchsrechte; elektronische Einwilligung	Nutzung eines Webangebotes
Ebene 3: Inhaltsebene **Rechtsgrundlage:** "Offline-Recht"; BDSG, Landesdatenschutzgesetze	Ergeben sich aus dem Fachrecht und den jeweiligen Datenschutzgesetzen	Melderegisterauskunft; Anforderung von Briefwahlunterlagen; Anwohnerparkausweis

- **Ebene 1: Transportebene**: Damit ein Tele- oder Mediendienst angeboten und ein Nutzer ihn in Anspruch nehmen kann, muss eine technische Verbindung zwischen Anbieter und Nutzer hergestellt werden. Hierzu bedient man sich der Dienste eines Telekommunikationsdiensteanbieters. Bei der Bereitstellung der notwendigen TK-Dienste fallen beim TK-Diensteanbieter Bestands-, Verbindungs- und Abrechnungsdaten an. Beim Umgang mit diesen Daten hat der TK-Diensteanbieter das TKG (§§ 85 und 89) und die TDSV zu beachten.

- **Ebene 2: Transportbehälterebene:** Greift nunmehr der Nutzer unter Verwendung der Telekommunikationsverbindung auf das Angebot des Tele- oder Mediendiensteanbieters zu, wird die zweite Schicht, nämlich die Transportbehälterebene berührt. Der Tele- bzw. der Mediendiensteanbieter benötigt für das Bereitstellen seines Dienstes vom Nutzer eine Reihe von personenbeziehbaren Daten und erhebt weitere Daten im Zusammenhang mit der Nutzung des Dienstes. Es fallen also Bestands-, vorgangsbezogene Nutzungs- und Abrechnungsdaten des Nutzers an. Der rechtmäßige Umgang mit diesen Daten und die Rechte der Nutzer sind im TDG, im TDDSG und im MDStV geregelt:
- **Ebene 3: Inhaltsebene**. Wenn ein Tele- oder Mediendienst genutzt wird, werden hierbei Informationen und vielfach auch personenbezogene Daten an den Nutzer weitergegeben oder ausgetauscht. Der Nachrichteninhalt ist in einer eigenen Schicht mit vielfältigen Rechtsvorschriften geregelt. Für den Inhalt der Kommunikation sind die Telekommunikation und die Tele- und Mediendienste nur „Trägermedien". Zunächst gilt entsprechend dem Gegenstand der betreffenden E-Government-Anwendung das jeweilige Fachrecht (Inhaltsebene = Offline-Recht); so gilt zum Beispiel für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten bei einer elektronischen Melderegisterauskunft das jeweilige Landesmelderecht. Soweit das Fachrecht keine bereichsspezifischen Regelungen zum Datenschutz enthält, gelten die Regelungen des jeweiligen Landesdatenschutzgesetzes.

Diese Dreiteilung bei den anzuwendenden Datenschutzregelungen, anhand derer die Konkretisierung der jeweils einschlägigen datenschutzrechtlichen Anforderungen vorzunehmen ist, gilt entsprechend bei allen E-Government-Anwendungen."

5.7.2 Welche grundsätzlichen Anforderungen bestehen für die Erhebung und Verarbeitung von personenbezogenen Daten?

Die Erhebung und Verarbeitung personenbezogener Daten bedarf immer entweder einer **gesetzlichen Ermächtigung**, die die Erhebung, Speicherung, oder Nutzung von personenbezogenen Daten erlaubt oder der **ausdrücklichen Einwilligung des Betroffenen**. Das Erfordernis der datenschutzrechtlichen Einwilligung besteht also nur dann, wenn eine Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten über den gesetzlichen gestatteten Umfang (vgl. §§ 5, 6 TDDSG) hinausgehen soll. Ansonsten ist die Unterrichtung des Nutzers über die Verwendung seiner personenbezogener Daten nach Maßgabe des § 4 Abs. 1 TDDSG ausreichend. In den Landesdatenschutzgesetzen (LDSG) finden sich regelmäßig die Anforderungen an eine rechtswirksame Einwilligung des Betroffenen. Hiernach muss die Einwilligung freiwillig erfolgen, der Betroffene über Umfang und Folgen der Einwilligung aufgeklärt werden, der Schriftform genüge getan sein und der Betroffene über die Widerrufbarkeit seiner Einwilligung aufgeklärt werden.

5.7.3 Wie kann eine datenschutzrechtliche Einwilligung online erfolgen?

Grundsätzlich besteht für eine datenschutzrechtliche Einwilligung das Erfordernis der Schriftform. Auch diesem Schriftformerfordernis kann auf elektronischem Weg entsprochen werden. Hierfür ist allerdings zwischen einer Einwilligung zur Erhebung von **Nutzungsdaten** und einer Einwilligung zur Erhebung von **Inhaltsdaten** zu differenzieren:

- Für das Angebot von Telediensten bzw. Mediendiensten und eine hiermit verbundene Erhebung von personenbezogenen Daten ohne gesetzliche Grundlage, reicht eine elektronische Einwilligung i.S.v. § 4 Abs. 2 TDDSG bzw. § 18 Abs. 2 MDStV aus. Diese gesetzlichen Vorgaben erfordern explizit **keine qualifizierte elektronische Signatur** im Sinne des Signaturgesetzes (SigG). Die elektronische Einwilligung kann somit online als auch per E-Mail erfolgen. Dies gilt jedoch nur für die Verarbeitung solcher Daten, die im unmittelbaren Zusammenhang mit dem jeweiligen Tele- bzw. Mediendienst stehen, also für **Nutzungsdaten**.
- Für eine Datenverarbeitung der **Inhaltsdaten** findet dagegen das Schriftformerfordernis des § 4a Abs. 1 S. 2 BDSG / bzw. der entsprechenden LDSG Anwendung. Dies hat zur Folge, dass dann auch für die elektronische Einwilligung gem. § 126a BGB eine qualifizierte elektronische Signatur notwendig ist, um dem Schriftformerfordernis zu entsprechen.

5.7.4 Was folgt aus dem Grundsatz der Datenvermeidung und Datensparsamkeit?

Der **Grundsatz der Datenvermeidung und der Datensparsamkeit** besagt, dass sich die Gestaltung und Auswahl elektronischer Dienste an dem Ziel auszurichten hat, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Die Verwaltung hat also schon bei der Ausgestaltung der elektronischen Verwaltungsprozesse, datenvermeidende und datensparsame Alternativen zu wählen. Aufgrund der Geltung des Grundsatzes der Datenvermeidung und der Datensparsamkeit geben die Datenschutzbeauftragten des Bundes und der Länder folgende Hinweise:

- „Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass sie ohne personenbezogene Daten durchgeführt werden können.
- Der Datenverarbeitungsprozess ist so zu organisieren und die Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass die Verarbeitung personenbezogener Daten minimiert wird, indem weitgehend auf einen Personenbezug verzichtet wird.
- Insbesondere ist auf eine Identifizierung der Betroffenen zu verzichten, soweit dies nicht rechtlich gefordert wird.
- In den Fällen, in denen es nur auf eine Berechtigung (z.B. Gebühr bezahlt) oder eine bestimmte Eigenschaft (z.B. Arzt) ankommt, ist nur deren Vorliegen zu prüfen und auf die Identifizierung des Handelnden zu verzichten.
- Soweit technisch möglich und zumutbar, ist den Betroffenen zu ermöglichen, anonym oder pseudonym zu handeln.
- Soweit technisch möglich und zumutbar, ist den Betroffenen zu ermöglichen, anonym oder pseudonym zu bezahlen. Hierfür können unterschiedliche Zahlungsverfahren genutzt werden, die diese Möglichkeit bieten."

5.7.5 Was folgt aus dem Grundsatz der Zweckbindung?

Zum **Grundsatz der Zweckbindung** stellte das BVerfG im "Volkszählungsurteil" fest, dass ein Zwang zur Angabe personenbezogener Daten voraussetzt, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Hieraus folgt, dass die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken unzulässig ist. **Die Verwendung der Daten ist also auf den gesetzlich bestimmten Zweck begrenzt**. Liegt kein die Erhebung begründendes Gesetz vor, ist daher die persönliche Zustimmung des Betroffenen zur Datenerhebung und Bearbeitung notwendig. Eine einfachgesetzliche Regelung der Zweckbindung findet sich für Fälle der Datenverarbeitung öffentlicher Stellen in § 14 Abs. 2 BDSG und für die Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen in den §§ 28, 29, 30, 3, 39 BDSG. Eine Regelung der Zweckbindung enthält auch das Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz –TDDSG), welches gem. § 2 Nr. 1 TDDSG für alle Teledienstеanbieter gilt, unabhängig davon, ob sie öffentlich-rechtlich oder privatrechtlich organisiert sind. Gem. § 3 Abs. 2 TDDSG darf der Diensteanbieter für die Durchführung von Telediensten erhobene personenbezogene Daten für andere Zwecke nur verarbeiten und nutzen, soweit das TDDSG oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

5.7.6 Was folgt aus dem Grundsatz der Erforderlichkeit?

Die Datenschutzbeauftragten des Bundes und der Länder führen zum Grundsatz der Erforderlichkeit aus: "Die Einhaltung des Erforderlichkeitsgrundsatzes im Einzelfall ist bereits in der Konzeptions- und Planungsphase von E-Government-Anwendungen und bei der Systemauswahl zu berücksichtigen. Insofern korrespondiert die Vorgabe mit den Geboten zur Datenvermeidung und -minimierung. Das Gebot der Erforderlichkeit gilt für alle Phasen der Verarbeitung, also nicht nur für die Erhebung, sondern auch für den gesamten anschließenden Verarbeitungsprozess. Daten, die für den weiteren Verwaltungsvollzug ab einer bestimmten Stufe nicht (mehr) erforderlich sind, sind zu löschen

oder, wenn sie für bestimmte Kontroll- oder Nachweisfunktionen im Einzelfall noch benötigt werden, zu anonymisieren oder zumindest zu pseudonymisieren. Diese Maßnahmen können von modernen DV-Systemen dynamisch durchgeführt werden, d.h. bei Überschreiten eines bestimmten Termins (Löschfrist, Antragsende, Ablauf der Wirkung eines Verwaltungsaktes) oder bei Eintritt eines bestimmten Ereignisses (der geforderte Nachweis wird erbracht) werden entsprechende Datenfelder gelöscht."

Schon im Vorfeld kann also durch **eine datenschutzgerechte Systemgestaltung** die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf das geringste notwendige Niveau reduziert werden. Eine gesetzliche Normierung hat dieser Grundsatz in § 3a Bundesdatenschutzgesetz (BDSG) erfahren. Eine Legaldefinition der Begriffe "Anonymisierung" und "Pseudonymisierung" findet sich in § 3 Abs. 6 u. 6a BDSG. Entsprechende Regelungen finden sich auch in den jeweiligen Datenschutzgesetzen der einzelnen Bundesländer. Hinsichtlich einer Berücksichtigung des Grundsatzes der Erforderlichkeit geben die Datenschutzbeauftragten des Bundes- und der Länder folgende Empfehlungen (in Auszügen):

- „Der Umfang der personenbezogenen Daten, die bei einer E-Government-Anwendung erhoben, verarbeitet und genutzt werden sollen, ist in einer verbindlichen Regelung vorab festzulegen.
- Angebote, bei denen eine persönliche Identifikation des Bürgers bzw. der Bürgerin nicht erforderlich ist (z. B. Formularabruf), müssen ohne Erhebung der Identifikationsdaten genutzt werden können.
- Bei reinen Informationsangeboten sollte auf eine vollständige Erfassung der IP-Adressen der Nutzer verzichtet werden, da diese für die Erbringung des Angebots und seine Abrechnung nicht erforderlich sind. Für die statistische Auswertung reichen gekürzte IP-Adressen aus.
- Bei E-Mail-Newslettern reicht die Erhebung der E-Mail-Adresse der Empfänger aus; die Erfassung des Namens und der postalischen Anschrift kann unterbleiben.
- Bei E-Government-Dienstleistungen dürfen nur diejenigen Nutzungsvorgänge protokolliert werden, bei denen dies aufgrund gesetzlicher Vorgaben erforderlich ist (z.B. automatisierte Abrufverfahren). Darüber hinaus dürfen Daten dann gespeichert werden, wenn konkrete Anhaltspunkte für eine missbräuchliche Inanspruchnahme vorliegen und soweit die Daten zur Missbrauchsaufklärung erforderlich sind. Diese Daten dürfen nicht für andere Zwecke genutzt werden.
- Elektronische Erhebungsformulare sind so zu gestalten, dass im Regelfall nur diejenigen Daten abgefragt werden, die für die jeweilige Aufgabe erforderlich sind. Sofern auch „Überschussdaten" erhoben werden, ist ausdrücklich auf die Freiwilligkeit der entsprechenden Angaben hinzuweisen. Bei der Übernahme analoger Formulare im Rahmen von e-Government-Anwendungen ist vorab besonders kritisch zu prüfen, ob wirklich alle bisher erhobenen Daten für die Aufgabenerledigung der Verwaltung erforderlich sind. (...)"

5.7.7 Was folgt für die Verwaltung aus dem Grundsatz der informationellen Gewaltenteilung

Der **Grundsatz der informationellen Gewaltenteilung** ergibt sich aus den bereits dargestellten Grundsätzen der Zweckbindung und Erforderlichkeit. Jede Verwaltungsstelle soll nur Zugriff auf die für ihre Aufgabenerfüllung erforderlichen Daten haben. Bei dem Betrieb einer zentralen Kommunikationsstelle (virtuelle Poststellen; virtuelle multifunktionale Bürgerbüros, Mail-Provider) ist hiernach darauf zu achten, dass die Administratoren der zentralen Kommunikationsstellen keinen Zugang zu sensiblen sog. "Inhaltsdaten" erhalten, die nur einem bestimmten anderen Empfänger vorbehalten sind. Dieses „**Abschottungs-Prinzip**" gilt auch für Untereinheiten größerer Stellen. Der Grundsatz der informationellen Gewaltenteilung wird insbesondere dort relevant, wo eine Bündelung des Zugangs zu verschiedensten Verwaltungstätigkeiten unterschiedlicher Verwaltungsträger in einer Stelle stattfindet. Er ist von besonderer Bedeutung, soweit die eingehenden Daten besonderen gesetzlichen Geheimhaltungserfordernissen unterliegen (z.B. im Bereich der Steuer- und Sozialverwaltung). Eine Organisation von zentralen Kommunikationstellen sollte daher eine **strikte Trennung von Nutzungs- und Inhaltsdaten** gewährleisten (durch gesetzliche Regelungen oder klare Dienstanweisungen). Siehe zur datenschutzgerechten Gestaltung von "Virtuellen Poststellen" S. 50.

5.7.8 Welcher Anspruch besteht für den Betroffenen hinsichtlich Berichtigung, Löschung oder Sperrung personenbezogener Daten?

Hierzu führen die Datenschutzbeauftragten des Bundes und der Länder folgendes aus: "Zu den Korrekturrechten der Betroffenen gehört der Anspruch auf Berichtigung, Löschung und Sperrung der zu ihrer Person gespeicherten Daten. Unrichtige Daten beeinträchtigen das Recht auf informationelle Selbstbestimmung genauso wie unrechtmäßig erhobene Daten und sind daher unverzüglich zu berichtigen. Die Pflicht zur Berichtigung besteht unabhängig davon, ob der Betroffene einen Anspruch geltend macht.
Die speichernde Stelle hat die Daten zu löschen, wenn die Speicherung nicht zulässig oder für die Aufgabenerfüllung nicht mehr erforderlich ist. Dabei bedeutet Löschen das Unkenntlichmachen von Daten, so dass sie für niemanden mehr zugänglich sind. Die Löschung hat unverzüglich, d.h. ohne schuldhaftes Zögern, zu erfolgen. Wenn Aufbewahrungspflichten bestehen oder wenn anzunehmen ist, dass schutzwürdige Interessen des Betroffenen durch die Löschung beeinträchtigt werden, tritt an die Stelle der Löschung eine Sperrung.
Daten sind außerdem zu sperren, wenn ihre Richtigkeit nicht eindeutig ist oder die Sperrung von dem Betroffenen verlangt wird. Darüber hinaus haben Betroffene die Möglichkeit, einer an sich rechtmäßigen Datenverarbeitung aus besonderen schutzwürdigen persönlichen Gründen zu widersprechen. Der Widerspruch zwingt die verantwortliche Stelle, die beabsichtigte Datenverarbeitung im Hinblick auf die vom Betroffenen geltend gemachte besondere persönliche Situation zu überprüfen."

5.7.9 Welche datenschutzrechtlichen Vorgaben bestehen für eine virtuelle Poststelle der Verwaltung?

Hierzu führen die Datenschutzbeauftragten des Bundes und der Länder folgendes aus: "(...) Grundsätzlich soll die Virtuelle Poststelle **keine Kenntnis der Inhalte** der Kommunikation erhalten. Daher erfolgt eine Adressierung über Zertifikatsinhalte oder andere Metainformationen über die Dokumente, die eine Weiterleitung ohne Zeitverzögerung an die zuständige Stelle (z.B. Sozialamt, Meldeamt) ermöglichen. Die Virtuelle Poststelle als Basiskomponente "Datensicherheit" fungiert als zentrales E-Mail-Gateway und Dienstleister für Web-Applikationen zur Sicherstellung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation zwischen Bürgern und Verwaltung. Es wird daher empfohlen:

- Das Personal des beauftragen Unternehmens ist auf das Datengeheimnis (z.B. nach § 5 BDSG) zu verpflichten.
- Die Virtuelle Poststelle erhält keine Kenntnis von den Inhalten der Kommunikation. Dies kann bspw. durch "elektronische Briefumschläge" für die Inhaltsdaten, wie etwa nach dem OSCI-Standard, sichergestellt werden. Die Zuordnung zur fachlich zuständigen Stelle erfolgt über Zertifikatsdaten (Signatur-, Verschlüsselungs- oder Authentisierungszertifikat) bzw. andere Metainformationen, die den eigentlichen Inhaltsdaten beigefügt sind.
- Es dürfen jeweils nur die erforderlichen Daten an das Back-End weitergegeben werden.
- Die Inhaltsdaten müssen sowohl im Post-Eingangsbereich als auch bei der Weiterleitung an die fachlich zuständige Stelle gegen unberechtigte Zugriffe geschützt werden. Mit der Virtuellen Poststelle wird sichergestellt, dass eine automatisierte Weiterleitung der Bürgerkontakte an die fachlich zuständige Stelle ohne inhaltliche Auswertung durch die übergreifende „Poststelle" erfolgt.
- Die Zuordnung der jeweiligen Vorgänge zu einer elektronischen Akte sollte nicht durch die virtuelle Poststelle, sondern durch die fachlich zuständige Stelle erfolgen. Nur sie kann letztlich die Relevanz der entsprechenden Informationen beurteilen und ihre genaue fachliche Zuordnung vornehmen.
- Zwischen jeder Fachstelle und einem zentralen Portal ist ein eigenes Auftragsverhältnis zu begründen und durch schriftliche Festlegungen abzusichern."

5.7.10 Was ist aus datenschutzrechtlicher Sicht bei der Speicherung von Grunddaten des Bürgers zu beachten?

Die Datenschutzbeauftragten des Bundes und der Länder führen hierzu aus: "Die häufigere Nutzung elektronischer Bürgerdienste kann dazu führen, dass jemand seinen Namen, seine Anschrift sowie weitere in anderen Zusammenhängen relevante Grunddaten immer wieder neu in die entsprechenden Eingabemasken eintragen muss. Um den

Bürgerinnen und Bürger diese immer wiederkehrende Erfassung abzunehmen, kann ihnen die Möglichkeit geboten werden, dass Daten, die einmal erfasst worden sind, automatisch für die Bürgerdienste übernommen werden. Technisch können diese Daten auf einer Chipkarte des Bürgers gespeichert, auf dessen PC oder in einem besonderen Bereich des Internetportals hinterlegt werden. Eine dezentrale Lösung ist unter dem Gesichtspunkt, das Entstehen zentraler Datensammlungen möglichst zu vermeiden, vorzuziehen." Hieraus ergeben sich folgende Handlungsempfehlungen der Bundes- und Landesdatenschutzbeauftragten:

- "Niemand kann dazu gezwungen werden, Daten auf Vorrat für Bürgerdienste zu hinterlegen.
- Die Erfassung, Änderung oder Löschung dieser Daten darf nur nach einer zuverlässigen Authentifizierung des Bürgers möglich sein. Die übertragenen Daten sind durch Verschlüsselung vor unberechtigter Kenntnisnahme und Verfälschung zu schützen.
- Es sollte stets die Möglichkeit geboten werden, die für die Nutzung eines konkreten Bürgerdienstes erforderlichen Daten erst im jeweiligen Einzelfall einzugeben.
- Der Bürger sollte frei darüber entscheiden können, welche Datenarten er für künftige Nutzungen hinterlegt.
- Die Speicherung sollte so erfolgen, dass nur die Bürger selbst auf die von ihnen hinterlegten Daten zugreifen und deren Transfer in einzelne Bürgerdienste veranlassen können.
- Der Bürger sollte die von ihm hinterlegten Daten jederzeit einzeln oder insgesamt löschen können. Um Datenfriedhöfe zu vermeiden, sollten hinterlegte Daten, die über eine längere Zeit hinweg nicht mehr genutzt wurden, automatisch gelöscht werden. Soweit der betreffende Bürger eine E-Mail-Adresse hinterlegt hat, kann er rechtzeitig vor der automatischen Löschung darüber informiert und ihm die Möglichkeit gegeben werden, die Löschung zu verhindern.
- Sofern die Daten in Chipkarten oder auf dem PC der Anwender hinterlegt werden sollen, sollten die Dienststellen, die von diesen Daten Gebrauch machen wollen, ein Sicherheitskonzept erarbeiten, das auch berücksichtigt, wie die in der Sphäre der Bürger gespeicherten Daten vor unberechtigten Zugriffen sowie vor Manipulation geschützt werden können."

Weiterführende Literatur:
Zu Fragen des Datenschutzes im Ganzen LfD Niedersachsen (Hrsg.), „Datenschutz gerechtes eGovernment" Dezember 2002 (zu Praxisbeispielen S. 72 ff.);
Zur elektronischen Einwilligung im Internet: *Rasmussen*, Die elektronische Einwilligung im TDDSG, DuD 2002, S. 406ff; *v.Lewinski*, Privacy Policies: Unterrichtung und Einwilligung im Internet, DuD 2002, S. 395 (398f.); *Schaar*, Datenschutzrechtliche Einwilligung im Internet, MMR 2001, S. 644ff.; *ders.* Datenschutz im Internet, 2002, S. 178ff.; *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, 2003, S. 160ff. Zu Mitarbeiterdaten im Internet und Fragen der Einwilligung: *Gola*, Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 2002, S. 109ff.

5.8 Welche rechtlichen Vorgaben sind hinsichtlich der Gleichstellung von Behinderten zu berücksichtigen?

Eine Verpflichtung zur Berücksichtigung der Bedürfnisse von Personen mit Behinderungen bei der Gestaltung von Online-Angeboten ergibt sich für die Bundesverwaltung aus dem neu erlassenen **Gesetz zur Gleichstellung behinderter Menschen** (Behindertengleichstellungsgesetz – BGG) vom 27. April 2002 (BGBl. I S. 1467) und der aufgrund der Ermächtigung in § 11 Abs. 1 BGG erlassenen **Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz** (Barrierefreie Informationstechnik-Verordnung – BITV vom 17. Juli 2002, BGBl. I 2002, S. 2645). Es ist zu erwarten, dass die Länder bald entsprechende Gesetze verabschieden.

5.8.1 Was folgt aus dem Gesetz zur Gleichstellung behinderter Menschen?

Das Behindertengleichstellungsgesetz hat zum Ziel, die gleichberechtigte Teilhabe von behinderten Menschen am Leben in der Gesellschaft zu gewährleisten und ihnen eine selbstbestimmte Lebensführung zu ermöglichen (vgl. § 1 BGG). Es gilt für Dienststellen und sonstige Einrichtungen der Bundesverwaltung, einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Auch Landesverwaltungen, einschließlich der landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, werden vom Geltungsbereich des Gesetzes erfasst, soweit sie Bundesrecht durchführen. Mit § 11 BGG verpflichtet sich der Bund zu einer barrierefreien Gestaltung seiner Internetangebote. Internetauftritte und -angebote sowie die zur Verfügung gestellten grafischen Programmoberflächen, die mit Mitteln der Informationstechnik dargestellt werden, sind so zu gestal-

ten, dass sie von behinderten Menschen grundsätzlich uneingeschränkt genutzt werden können.

5.8.2 Was folgt aus der Barrierefreie Informationstechnik-Verordnung?

Die konkret anzuwendenden technischen Standards, die zu gestaltenden Bereiche und Arten amtlicher Information sowie die einzubeziehenden Gruppen behinderter Menschen, wurden in der Barrierrefreie Informationstechnikverordnung (BITV) festgelegt. Die technischen Details zur Umsetzung finden sich in einer nach Prioritäten aufgeteilten Anlage zur Rechtsverordnung. Gegenstand der BITV sind lediglich **öffentlich zugängliche Internetangebote**. Nicht umfasst von den gesetzlichen Vorgaben des BGG und der BITV sind daher elektronisch bereitgestellte Informationen, die ausschließlich innerhalb der Verwaltung z.B. über das verwaltungsinterne Intranet den Verwaltungsbediensteten zugänglich gemacht werden.

5.8.3 Enthält auch das SGB IX Vorgaben für die Verwaltung?

Die sich unter bestimmten Voraussetzungen aus dem neunten Sozialgesetzbuch (SGB IX) ergebenen Ansprüche des Arbeitnehmers auf einen barrierefreien Zugang zu Angeboten des Internets gelten auch für Arbeitnehmer in der öffentlichen Verwaltung unmittelbar. Für Beamte erhalten sie über § 128 SGB IX Geltung.
Gem. § 33 Abs. 3 Nr. 1 und 6 i.V.m. Abs. 8 Nr. 5 SGB IX können barrierefreie Zugänge zum Internet als Leistung zur Teilhabe am Arbeitsleben **(technische Arbeitshilfen)** qualifiziert werden. Ebenso können für schwerbehinderte Arbeitnehmer solche Leistungen als technische Arbeitshilfe gem. § 102 Abs. 3 Nr. 1a SGB IX erbracht werden. Auf erforderliche technische Arbeitshilfen sowie auf eine behindertengerechte Einrichtung des Arbeitsplatzes im oben genannten Sinne haben **schwerbehinderte Menschen einen Anspruch gegen ihren Arbeitgeber gem. § 81 Abs. 4 S. 1 Nr. 4 und 5 SGB IX**. Allerdings wird der Anspruch des Arbeitnehmers durch die notwendige Zumutbarkeit für den Arbeitgeber begrenzt.
Auch innerhalb der Binnenstruktur der Verwaltung werden die Grundanforderungen an einen barrierefreien Zugang zum Internet daher immer beachtlicher, da auch hier der barrierefreie Zugang zu gewährleisten ist, wenn er für die Ausübung der beruflichen Tätigkeit notwendig ist. Teilweise beziehen daher die Gesetzentwürfe einzelner Länder die barrierefreie Gestaltung auch des Intranets für die Landesverwaltungen explizit mit ein (vgl. z.B. Art. 13 des Entwurfes eines Bayerischen Behindertengleichstellungsgesetzes – BayBGG – Stand: 19.07.2002).

Weiterführende Literatur:
Hellbusch, Barrierefreies Webdesign – wie Menschen mit Behinderungen WWW-Seiten lesen können, Knowware-Verlag, Oktober 2001. Eine umfangreiche Übersicht mit den Gesetzes- und Verordnungstexten sowie Hinweisen zur Erstellung barrierefreier Internetseiten werden durch das Forschungsinstitut Technologie-Behindertenhilfe der Fernuniversität Hagen online unter www.fernuni-hagen.de/FTB bereitgehalten. Weitere Hinweise zur Erstellung eines barrierefreien Webdesigns können online unter www.barrierefreies-webdesign.de abgerufen werden.

5.9 Welche Anbieterpflichten folgen für das Angebot der Verwaltung aus der Qualifizierung als öffentliche Einrichtung?

5.9.1 Wann sind das Portal oder einzelne Portalangebote als öffentliche Einrichtung zu qualifizieren?

Sowohl das Portal als auch einzelne Dienstleistungen auf dem Portal können grundsätzlich öffentliche Einrichtungen bilden. Denn der kommunalrechtliche Begriff der öffentlichen Einrichtung umfasst Leistungsapparaturen höchst unterschiedlicher Struktur und Zweckbestimmung, denen letztlich nur die Funktionsweise gemeinsam ist, die Voraussetzungen für die Daseinsfürsorge und Daseinsvorsorge der Bevölkerung zu schaffen und zu gewährleisten. Dabei verliert eine Einrichtung den Charakter als öffentliche Einrichtung nicht, wenn sie gleichzeitig als wirtschaftliches Unternehmen eingeordnet werden muss.
Eine Einordnung als öffentliche Einrichtung setzt grundsätzlich einen Widmungsakt voraus. Dieser kann ausdrücklich (durch Ratsbeschluss, eine vom Gemeinderat zu beschließende Satzung oder administrativ), aber auch konkludent z.B. durch die faktische Indienststellung erfolgen. Maßgeblich ist die Erkennbarkeit des Willens der Verwaltung, der auch aus Indizien (Zweck, geäußerte Absicht, Zulassungspraxis, Gebühren, Benutzungsordnung) abgeleitet werden kann. Im Hinblick auf die städtischen Portale können dafür z.B. die tatsächliche Zulassungspraxis oder die politisch geäußerten Zwecke des Portals hinzugezogen werden. Im Hinblick auf einen kommunalen Betrieb in öf-

fentlicher oder privatrechtlicher Rechtsform hat die Rechtsprechung die Vermutungsregel entwickelt, dass für die Allgemeinheit nutzbare kommunale Einrichtungen „öffentliche" Einrichtungen sind. Die Gemeinde kann die Vermutung durch den Nachweis widerlegen, die Bereitstellung erfolge ausdrücklich als private Einrichtung.
Soweit **Private oder ein gemischtwirtschaftliches Unternehmen Betreiber** des Portals sind, bedarf eine Widmung der Zustimmung des Privaten. Dies kann z.B. der Fall sein, wenn vertraglich (Betreibervertrag) die Gemeinwohlverpflichtung festgelegt wird, u.a. durch die Verpflichtung, allen Einwohnern die Nutzung kostenlos oder zu einem bestimmten Entgelt zu eröffnen.

5.9.2 Welche Ansprüche haben die Einwohner bei einer Einordnung als öffentliche Einrichtung?

Eine **Qualifikation als öffentliche Einrichtung** vermittelt nach den Gemeindeordnungen allen Einwohnern, Unternehmen und Einrichtungen des Gemeindegebiets einen Rechtsanspruch, das Portal oder einzelne Portalangebote im Rahmen ihres Widmungszwecks unter Beachtung des **Gleichheitsgrundsatzes** (Art. 3 Abs.1 GG) zu nutzen. Auch der generelle Vorrang eigener Reservierungswünsche der Kommune auf dem Portal, ohne sachgerechtes Differenzierungskriterium, ist unzulässig. Allerdings können sich sachgerechte Erwägungen aus den verfolgten öffentlichen Zwecken und dem damit zusammenhängenden Widmungszweck ergeben.
Der Zulassungsanspruch wird aber begrenzt durch **den Nutzungszweck**, der damit auch die Nutzungsgrenzen festlegt. Für Stadtportale ergibt sich daraus in der Regel das Recht, auf Zugang der Einwohner zu den auf dem Portal angebotenen Dienstleistungen sowie das Recht, auf dem Portal als Anbieter von Dienstleistungen präsent zu sein. **Nutzungsgrenzen** können sich ferner v.a. aufgrund von **Kapazitätsengpässen** ergeben. Denn die Gemeinde ist nicht verpflichtet, bei Engpässen neue Kapazitäten aufzubauen oder vorhandene Einrichtungen im bisherigen Umfang aufrechtzuerhalten. Soweit das Portal an Kapazitätsgrenzen stößt, ist das Gebot sachgerechter Bewerberauswahl unter Berücksichtigung von Art. 3 Abs.1 GG zu beachten. Zulässig ist regelmäßig u.a. das Prioritätsprinzip. Es empfiehlt sich, die Grundsätze für die Einschränkung des Zulassungsanspruchs in Form von allgemeinen vom Gemeinderat beschlossenen Richtlinien festzulegen und auf dem Portal zu veröffentlichen. Die Verwaltung hat die Art der Nutzung näher zu regeln und Störungen von der Einrichtung fernzuhalten („Hausrecht"). Es empfiehlt sich, die für den reibungslosen Betrieb der Einrichtung erforderlichen Pflichten in Form von Nutzungsbedingungen zu regeln und auf dem Portal zu veröffentlichen. Hieraus ergeben sich zahlreiche konkrete Regelungs- und Eingriffsbefugnisse (vgl. S. 45).

Weiterführende Literatur und Rechtsprechung:
Allgemein: *Schmidt-Aßmann*, in: ders. (Hrsg.) Besonderes Verwaltungsrecht, 11. Aufl. 1999, 1. Abschn. Rnr. 105ff.*; Erichsen*, Die kommunalen öffentlichen Einrichtungen, Jura 1986, S. 148 und S. 196. Zur Widmung als öffentliche Einrichtung bei privatem Betrieb: *VGH München*, NVwZ-RR 1999, S. 197.

5.10 Was ist grundsätzlich bei Dienstanweisungen oder Betriebsvereinbarungen für den Einsatz von Informtationstechnik am Arbeitsplatz zu beachten?

Für den Einsatz von Informationstechnik am Arbeitsplatz sind teilweise ergänzende Regelungen in Dienstanweisungen oder Betriebsvereinbarungen notwendig bzw. zur Steuerung des Verwaltungshandelns sinnvoll.

5.10.1 Für welche Bereiche ist eine Regelung durch Dienstanweisungen oder Betriebsvereinbarungen sinnvoll?

Eine Regelung durch Dienstanweisungen oder Betriebsvereinbarungen ist für solche Bereiche sinnvoll, in denen eine Beteiligung des Personal- oder Betriebsrates erforderlich ist. Eine notwendige Beteiligung des Personal- oder Betriebsrates bei Maßnahmen zur E-Government-gerechten Organisation in der Verwaltung ergeben sich **aus technik- und arbeitsplatzbezogenen Vorschriften**. Für öffentlich-rechtliche Einrichtungen des Bundes und der Länder enthält das Bundespersonalvertretungsgesetzes (BPersVG) bzw. die entsprechenden Landesgesetzgebungen und für private Betriebe das Betriebsverfassungsgesetz (BetrVG) relevante Regelungen.

- Das BPersVG sieht z.B. eine Zustimmung oder **Beteiligung des Pesonalrates** gem. § 75 Abs. 3 Nr. 16 u. Nr. 17 BPersVG für Angelegenheiten von Angestellten und Arbeitern über die **Gestaltung der Arbeitsplätze** sowie der Einführung und Anwendung technischer Ein-

richtungen zur Verhaltens- oder Leistungsüberwachung vor. Gem. § 76 Abs. 2 BPersVG hat der Personalrat ebenfalls bei Angelegenheiten von Beamten über **Maßnahmen zur Hebung der Arbeitsleistung und Erleichterung des Arbeitsablaufes** und der **Einführung grundlegend neuer Arbeitsmethoden** mitzubestimmen. Auch hat der Personalrat gem. § 75 Abs. 3 Nr. 11 BPersVG ein Mitbestimmungsrecht bei Maßnahmen zur Verhütung von Gesundheitsschäden. Letztlich können auch **datenschutzrelevante Maßnahmen** einer Pflicht zur Zustimmung des Personal- bzw. Betriebsrates unterfallen. Wird z.B. in einer Hochschule gestattet, personenbezogene Daten wissenschaftlicher Mitarbeiter über das Internet abrufbar bereitzustellen, so unterliegt dies dem Mitbestimmungsrecht des Personalrats.

- Der **Betriebsrat** hat gem. § 87 Abs. 1 Nr. 6 BetrVG ebenfalls ein Mitbestimmungsrecht, wenn technische Einrichtungen das Verhalten oder die Leistung von Arbeitnehmern überwachen können. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts (BAG) reicht es hierbei schon aus, wenn die technische Einrichtung lediglich objektiv zur Überwachung der Arbeitnehmer geeignet ist. Bereits ein bloßer Internetanschluss unterliegt aufgrund seiner Standardsoftware zur Nutzerprotokollierung daher nach h.M. dem Mitbestimmungsrecht durch den Betriebsrat. Des weiteren hat der Arbeitgeber gem. § 90 Abs. 1 BetrVG den Betriebsrat auch über **die Planung von technischen Anlagen, Arbeitsverfahren und Arbeitsabläufen** zu unterrichten und gem. § 90 Abs. 2 BetrVG die Vorschläge und Bedenken des Betriebsrats in seine Planung einzubeziehen. Dem Betriebsrat kommt letztlich auch unter den Voraussetzungen des § 91 BetrVG ein Mitbestimmungsrecht zu, wenn **Änderungen der Arbeitsplätze, des Arbeitsablaufes oder der Arbeitsumgebung** offensichtlich den gesicherten arbeitswissenschaftlichen Erkenntnissen über eine menschengerechte Arbeitsgestaltung widersprechen.

5.10.2 In wieweit ist neben der Personalvertretung auch der behördliche Datenschutzbeauftragte zu beteiligen?

Hierzu führen die Datenschutzbeauftragten des Bundes und der Länder aus: "Durch die Möglichkeiten der Inhaltskontrolle und Protokollierung in E-Government-Projekten können die einbezogenen Beschäftigten einer Verwaltung prinzipiell überwacht und ihre Leistung und ihr Verhalten kontrolliert werden. Deshalb ist es unerlässlich, eine Dienstvereinbarung mit der gewählten Personalvertretung abzuschließen, in der geregelt ist, was protokolliert wird, zu welchem Zweck Protokolldaten verwendet werden, wer Protokolle auswerten darf und wie lange Protokolle aufbewahrt werden". Zum Inhalt einer Dienstvereinbarung siehe weiter auch S. 55-56.

"Soweit die Protokollierung der Aufrechterhaltung der Datensicherheit dient, ist festzuhalten, dass diese in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze unterliegen. Der behördliche Datenschutzbeauftragte (bDSB) soll dazu beitragen, dass seine Behörde den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Der behördliche Datenschutzbeauftragte

- hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen,
- ist vor Einführung der entsprechenden IT-Verfahren u. a. durch Durchführung und Überprüfung des Ergebnisses der Vorabkontrolle nach den Regelungen des BDSG bzw. der entsprechenden Landesgesetze zu beteiligen,
- ist weiterhin zu beteiligen bei der Erstellung von Dienstanweisungen über getroffene bzw. zu treffende Datensicherungsmaßnahmen, bei Maßnahmen zum technisch-organisatorischen Datenschutz, bei der Auswertung von Protokolldateien, bei Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsverlangen und bei Bürgerbeschwerden mit Datenschutzbezug."

5.10.3 Welche Regelungsaspekte sollten von Dienstanweisungen bzw. Betriebsvereinbarungen umfasst werden?

Dienstanweisungen oder Betriebsvereinbarungen über die Nutzung elektronischer Kommunikationssystemen sollten inhaltlich beachten, dass

- der **Geltungsbereich und Zweck der Dienstanweisung/ der Betriebsvereinbarung** deutlich definiert ist;
- die **Zuständigkeiten und Verantwortungsbereiche** präzise dargestellt werden, insbesondere dort, wo es zu fach- oder amtsübergreifender Verantwortlichkeit kommt (z.B. Systembetreuer, Datenschutzbeauftragter);
- eine klare Darstellung des geplanten Einsatzes **(Nutzungskonzept)** erfolgt. In der Regel werden daher alle Formen der elektronischen Kommunikation, elektronische Aktenführung, die Verwendung von Signaturen als auch die Nutzung von Internet und Intranet hiervon umfasst sein;
- eine klare Definition der **Benutzungsbestimmungen der Kommunikationsmittel** erfolgt, z.B. das Verbot privater oder nicht mit dem System-Administrator abgestimmter Software, eine Vorgabe für die Zulässigkeit / Untersagung der privaten Nutzung etc.);
- ein umfassendes **Key-Management** die Verteilung und den Einsatz elektronischer Signaturen regelt (hierzu ausführlich unten S. 87);
- **Vorgaben für die E-Mail-Nutzung** gegeben werden, z.B. über Organisation des elektronischen Postfaches, Kenntlichmachung des Absenders etc. (hierzu ausführlich unten S. 63);
- **Maßnahmen zum Datenschutz und zur Datensicherheit** getroffen werden, z.B. über Zugangs- und Benutzerkontrollen, Passwortvergaben und die Verwahrung von Datenträgern.

Weiterführende Literatur:
Für die Beteiligung des Betriebsrates bzw. des Personalrates: *Naujock,* Internet-Richtlinien: Nutzung am Arbeitsplatz, DuD 2002 (Heft 26), S. 592ff. Zum Mitbestimmungsrecht des Personalrats bei Gestattung einer Hochschule, personenbezogene Daten wissenschaftlicher Mitarbeiter über das Internet abrufbar bereitzustellen: *OVG Nordrhein-Westfalen* v. 20.01.2000 – Akz.:1 A 128/98.PVL = JuRPC Web-Dok. 231/2000.
Praxisbeispiel: Musterdienstanweisung des Landesbeauftragten für Datenschutz Saarland für den Einsatz der Informationstechnik bei der Gemeinde, Stand 14.01.2002, abrufbar unter www.ifd.saarland.de/dschutz/MDAGem.htm.

6. Spezifische Vorgaben für die einzelnen Angebotstypen

Auf die reine E-Government-Tätigkeit der Verwaltung beschränkt, kann zwischen drei unterschiedlichen Angebotstypen unterschieden werden: Informations-, Kommunikations- und Transaktionsdienste. Grundsätzlich sind die Anforderungen technischer, organisatorischer und auch rechtlicher Art an Informationsdienste hierbei am geringsten und diese daher am ehesten zu realisieren. Die höchsten Anforderungen stellen sich an Transaktionsangebote der Verwaltung, da hier vollständig elektronisch auch komplexe Verwaltungsdienstleistungen rechtsverbindlich abgewickelt werden sollen. In der Regel beginnt die Verwaltung daher mit dem Angebot von Informationsdiensten und vertieft ihre Angebote dann über die Kommunikation bis zu vollständigen Transaktionsangeboten.

6.1 Was ist bei Informationsangeboten zu beachten?

Unter den Begriff der **elektronischen Informationsangebote** der Verwaltung wird hier die Bereitstellung elektronisch abrufbarer Information verstanden, ohne dass es zu einer individuellen Kommunikation zwischen Bürger und Verwaltung kommt. Der Bürger nimmt lediglich die passive Seite eines Informationsempfängers ein. Gleichwohl sind bereits für Informationsangebote der Verwaltung zahlreiche rechtliche Vorgaben zu beachten. Diese gehen jedoch zumeist nicht über solche Anforderungen hinaus, wie sie schon für die allgemeine Informationstätigkeit der Verwaltung in der „Offline-Welt" formuliert wurden. So dürfen bei dem Angebot von Informationsdienstleistungen die grundsätzlichen **Gebote der staatlichen Öffentlichkeitsarbeit** nicht überschritten werden. Eine Überschreitung liegt vor, wenn:

- Themen integriert werden, die **keinen Bezug zur Gemeinde** haben. Dies ist nach der Rechtsprechung des BVerfG z.B. der Fall, wenn der öffentliche bzw. kommunalpolitische Bezug der Äußerung fehlt und allgemeine politische und wirtschaftliche Nachrichten verbreitet werden.
- bei der Präsentation das Gebot der **Objektivität, Sachlichkeit und Transparenz nicht eingehalten** wird.

Besonders beachtlich sind aufgrund des hohen Verbreitungsgrades von Information über das Internet daneben die Vorgaben des Datenschutzes.

6.1.1. Welche datenschutzrechtlichen Vorgaben sind für Informationsdienste der Verwaltung zu beachten?

Grundsätzlich richtet sich die allgemeine Bereitstellung personenbezogener Daten im Internet nach den einschlägigen spezialgesetzlichen Regelungen. Sind solche nicht anwendbar, sind die Vorgaben des BDSG bzw. der LDSG zu beachten. Hieraus ergibt sich für die Nutzung personenbezogener Daten bei einer Informationstätigkeit der Verwaltung über das Internet nichts anderes, als dies bereits für die sonstige Informationstätigkeit der Verwaltung festgelegt wurde. Notwendig ist also eine Rechtsvorschrift, die eine solche Nutzung zulässt, oder die Einwilligung des Betroffenen (zu den Anforderungen einer Einwilligung und zur Zulässigkeit der elektronischen Einwilligung siehe oben S. 47).

Welche Besonderheiten gelten bei Informationsdiensten für personenbezogene Daten von Bediensteten?

Für die **personenbezogenen Daten von Bediensteten in** der Verwaltung kann sich durch Sonderregelungen in den Datenschutz- und Beamtengesetzen des Bundes bzw. der Länder eine Abweichung von den allgemeinen gesetzlichen Vorgaben ergeben. Diese sehen teilweise vor, dass eine Übermittlung von personenbezogenen Daten an Personen oder Stellen außerhalb des Dienstbereiches zulässig ist, wenn der Dienstverkehr es erfordert oder eine **Einwilligung des Betroffenen vorliegt**. Der Dienstverkehr erfordert in aller Regel die Bekanntgabe von personenbezogenen Daten wie Name, dienstlicher Telefon- und Fax-Nummer sowie Zuständigkeitsbereich und E-Mail-Adresse bei Bediensteten, die aufgrund ihrer Tätigkeit in der Verwaltung im erhöhten Maß mit Außenstehenden in Kontakt stehen (z.B. Ansprechpartner für Formen der Bürgerbeteiligung; Pressesprecher). Werden personenbezogene Daten von Bediensteten ins Internet eingestellt, kann dies teilweise auch die Mitbestimmung des Personalrats notwendig werden lassen (siehe zur Beteiligung des Personal- oder Betriebsrates auch oben unter S. 53).

Wie können Unsicherheiten bei der Verwendung von Bedienstetendaten vermieden werden?

Ist die Bestimmung des Zuständigkeitsbereiches unklar und die Anwendbarkeit der gesetzlichen Ermächtigung zweifelhaft, sollte eine **Einwilligung des Betroffenen** Bediensteten eingeholt werden. Auch sollte geprüft werden, ob zur Kontaktaufnahme mit der Behörde **anonymisierte E-Mail-Adressen** ausreichend sind. Auf Abbildungen der Bediensteten einer Verwaltung wird i.d.R. ganz verzichtet werden können. Da die Datenschutzbeauftragten einzelner Bundesländer für die Veröffentlichung von Bedienstetendaten immer eine Einwilligung des Betroffenen als rechtlich geboten ansehen, sollte letztlich bei Unklarheiten und nicht bestehender Einwilligung Rücksprache mit dem jeweiligen Datenschutzbeauftragten gehalten werden.

6.1.2. Wer haftet für Informationsinhalte?

Für welche Informationsinhalte auf dem Portal haftet die Verwaltung?

Für **eigene Informationen** haften die Betreiber des Stadtportals nach den allgemeinen Gesetzen (§ 8 TDG/§ 6 MDStV). Dazu gehören insbesondere die Verantwortlichkeit nach Haftungstatbeständen z.B. des Urheberrechtgesetzes (UrhG), Markengesetzes (MarkenG), Gesetzes gegen den unlauteren Wettbewerb (UWG) oder des Bürgerlichen Gesetzbuchs (BGB) sowie die strafrechtliche Haftung. Bei öffentlich-rechtlicher Ausgestaltung des Verhältnisses kommt regelmäßig auch eine der Amtshaftung (§ 839 BGB i.V.m. Art. 34 GG) in Betracht.
Sind die Rechtsbeziehungen privatrechtlich geregelt, kann für **leichte Fahrlässigkeit** die **Haftung** durch AGB grundsätzlich **ausgeschlossen** werden, soweit dies durch sachliche Gründe (z.B. Sicherung der Kostengünstigkeit der Leistungserbringung) gerechtfertigt ist sowie den Benutzern keine unverhältnismäßigen Opfer abverlangt werden und keine vertragswesentlichen Pflichten betroffen sind. Dasselbe gilt bei einer öffentlich-rechtlichen Ausgestaltung des Benutzerverhältnisses. Grenzen der Haftungsbeschränkung ergeben sich insoweit zusätzlich aus den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit. Allerdings ist die Verletzung von Pflichten aus einem verwaltungsrechtlichen Schuldverhältnis in der Regel zugleich auch eine Verletzung von Amtspflichten. Ob es bei öffentlich-rechtlicher Ausgestaltung des Benutzerverhältnisses letztlich zu einer Haftungsprivilegierung kommen kann, hängt daher davon ab, ob eine solche auch im Rahmen der Amtshaftung wirksam ist. Dies ist in Rechtsprechung und Literatur umstritten.
Sinnvoll ist bei der Informationsbereitstellung ein grundsätzlicher **Hinweis**, dass keine Haftung für die Richtigkeit und Vollständigkeit der Information übernommen wird.
Für **fremde Informationen**, die der Betreiber für einen Nutzer speichert, ist er grundsätzlich **nicht verantwortlich** (§ 11 TDG/ § 9 MDStV), wenn:

- er **keine Kenntnis von der rechtswidrigen Information** hat und ihm im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Information offensichtlich wird **oder**
- er **unverzüglich tätig geworden** ist, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald er diese Kenntnis erlangt hat.

Soweit sich der Betreiber aber **fremde Inhalte zu Eigen macht**, haftet er wie ein Autor der Informationen. Ein zu Eigen machen ist z.B. anzunehmen, wenn die fremden Informationen verändert werden. Es liegt aber auch schon dann vor, wenn die Darstellung auf den Durchschnittsempfänger wie eine eigene wirkt.
Auf den Portalseiten sollten bei Integration von fremden Inhalten daher immer **deutliche Hinweise** integriert werden, aus denen ersichtlich wird, dass es sich um fremde Informationen handelt.

Weiterführende Literatur:
Engels, Zivilrechtliche Haftung für Inhalte im World Wide Web, AfP 2000, S. 524ff.; Hoeren, Internetrecht, Stand: Oktober 2002, S. 341ff., abzurufen unter www.unimuenster.de/Jura.itm/hoeren/material/skript.pdf.

Besteht eine Haftung für rechtswidrige Inhalte in Hyperlinks?

Die Haftung für durch Hyperlinks vermittelte Inhalte ist durch die Rechtsprechung noch nicht abschließend geklärt. Entscheidend ist hier, wann durch das Hyperlinking ein zu Eigenmachen der fremden Informationen angenommen werden muss. Dabei hängt die rechtliche Beurteilung auch von **einer Betrachtung des Einzelfalles**, unter Berücksichtigung der Art des Hyperlinks, seiner Ausgestaltung und dem Kontext ab, in dem er gesetzt wird.
Erscheint nach Anklicken des Links die verknüpfte Seite im selben Gestaltungsrahmen der Ausgangsseite **(sog. „Frame-Links", „Inline-Links"**), wird dem Nutzer die ursprüngliche Fremdheit des Inhalts in der Regel nicht bewusst. In

diesem Fall besteht weitgehend Einigkeit, dass eine Haftung aufgrund eines zu-Eigen-machens angenommen werden muss.
Handelt es sich um einen „normalen" Hyperlink, bei dem die verlinkten Inhalte nicht in das eigene Angebot integriert werden, ist die haftungsrechtliche Einordnung in der Rechtsprechung umstritten. Teilweise wird von den Gerichten eine sehr weitgehende Haftung angenommen, die einer „Internetverkehrssicherungspflicht" gleichkommt. Jeder, der einen Link setze, mache sich den verlinkten Inhalt zu Eigen. Der Linksetzer gehe bewusst das Risiko ein, dass die Verweisungsseite später geändert wird und hafte daher bei ihrer Rechtswidrigkeit. Darüber hinausgehend wurde teilweise sogar eine Verantwortlichkeit für Hyperlinks, die lediglich über weitere Links zu rechtswidrigen Inhalten führten bejaht. Teilweise wird von den Gerichten aber auch die Ansicht vertreten, eine Haftung aufgrund eines zu Eigen Machens sei bei einfachen Hyperlinks nie gegeben, bzw. hänge immer von einer Betrachtung des Einzelfalles ab.
Aufgrund der **bestehenden rechtlichen Unsicherheit** bei der Haftung für Hyperlinks besteht die Gefahr, für rechtswidrige Inhalte auf den verlinkten Seiten in Anspruch genommen zu werden. Es wird daher empfohlen, bei Hyperlinks, die auf Internetseiten Dritter verweisen, Zurückhaltung zu üben. In jedem Fall sollte bei den Links ausdrücklich darauf hingewiesen werden, dass die verlinkten Inhalte nicht zu Eigen gemacht werden sowie zusätzlich eine Überprüfung der verlinkten Seiten in regelmäßigen Abständen stattfinden. Bei Kenntnisnahme über rechtswidrige Inhalte muss der Link unverzüglich beseitigt werden.

Weiterführende Literatur und Rechtsprechung:
Zur Internetverkehrssicherungspflicht*: OLG München*, MMR 2002, S. 625. Verlinkung über weitere Links*: LG Frankfurt*, CR 1999, S. 45. *Dippelhofer,* Verkehrssicherungspflicht für Hyperlinks? Anmerkung zum Urteil des OLG München vom 15. März 2002, 21 U 1914/02 (1), JurPC Web-Dok. 304/2002, Abs.1-22*; Köster/Jürgens*, Haftung professioneller Informationsvermittler im Internet, MMR 2002, S. 420ff..

6.1.3. Was ist bei der Integration fremder Informationsinhalte zu bedenken?

Ist für das Setzen von Hyperlinks die Zustimmung des Verlinkten erforderlich?

Die rechtliche Beurteilung dieser Frage ist noch nicht abschließend geklärt. Insbesondere ist immer eine konkrete **Betrachtung des Einzelfalles** notwendig, bei der die Art des Hyperlinks, seine Ausgestaltung sowie der Kontext, in dem er gesetzt wird, zu berücksichtigen sind.
Wird mit einem **„einfachen" Hyperlink** auf die Startseite eines anderen Anbieters verwiesen und die verweisende Seite bei Anklicken des Hyperlinks vollständig ersetzt, wird die Zustimmung regelmäßig als gegeben angenommen. Denn in der Errichtung einer Homepage wird gleichzeitig eine konkludente Zustimmung sowohl zur Verknüpfung mit Webseiten anderer über Hyperlinks als auch zu der darin liegenden Benutzungshandlung gesehen. Allerdings kann es im Einzelfall auch anders liegen. Bestehen Anzeichen, die gegen das vermutete Einverständnis sprechen, ist im Zweifel eine vorherige Zustimmung einzuholen.
Bei sog. **„Frame-Links" und "Inline-Links"** (vgl. S. 57) kann dagegen grundsätzlich nicht von einer konkludenten Zustimmung des Linksetzers ausgegangen werden. Bei einer fehlenden Zustimmung kommt eine Verletzung urheberrechtlicher- und wettbewerbsrechtlicher Vorschriften in Betracht. Eine Verletzung von § 13 UrhG kommt in Betracht, wenn der Hyperlink auf ein urheberrechtlich geschütztes Werk dazu führt, dass der Nutzer irrig annehmen muss, dieses sei dem Linksetzenden als Urheber zuzuordnen. Soweit ein **Wettbewerbsverhältnis** zwischen dem Betreiber und verlinktem Anbieter (z.B. regionales Portalangebot eines Privaten), kommen außerdem wettbewerbsrechtliche Verstöße gegen § 1 UWG, wenn zu Zwecken des Wettbewerbs das Arbeitsergebnis eines anderen unlauter angeeignet wird und gegen § 3 UWG aus dem Gesichtspunkt der Irreführung in Betracht. In diesen Fällen sollte eine **vorherige Zustimmung** eingeholt und ggf. eine Urheberbezeichnung eingefügt werden.
Führt der Hyperlink - unter Umgehung der Startseite gezielt auf darunter liegende Seiten **(sog. „Deep-Links"),** wird für den Nutzer durch die Anzeige der fremden Adresse und eines neuen Gestaltungsrahmens in der Regel deutlich, dass es sich um ein fremdes Angebot handelt. Sollte dies nicht der Fall sein, gelten die Ausführungen zu „Frame-Links" und „Inline-Links" entsprechend. Zusätzlich kann von einer konkludenten Zustimmung nicht ohne weiteres ausgegangen werden, da ggf. rechtlich relevante Hinweise oder auch die auf der Startseite geschaltete Werbung umgangen werden. Im Zweifel sollte daher die **vorherige Zustimmung** des Verlinkten eingeholt werden.
Darüber hinaus kommt eine **Markenrechtsverletzung** in Betracht, wenn die Verwendung der als Link verwendeten geschützten Bezeichnung den Eindruck erweckt, der Linksetzende kennzeichne damit eigene Leistungen. Vorausset-

zung für einen Anspruch aus §§ 14, 15 MarkenG hinsichtlich der Verwendung geschützter Marken und Kennzeichen als Links ist das Bestehen einer Verwechslungsgefahr. Links sollten deshalb optisch zurückhaltend gestaltet und als solche ausgewiesen sein.

Was ist bei der Einbindung sonstiger fremder Inhalte zu bedenken?

Werden beispielsweise **urheberrechtlich geschützter Werke** (z.B. Texte, Bilder, Grafiken oder Logos von Dritten) im Sinne von § 2 UrhG integriert, muss auf eine Lizenzierung dieser Werke zur Nutzung auf dem Internetportal geachtet werden. Daneben sind auch Datenbanken als schöpferische Leistung (§§ 2 Abs. 1 Nr.1 oder § 4 Abs. 2 UrhG) oder soweit für ihre Herstellung oder Erhaltung eine wesentliche Investition getätigt wurde (§§ 87 a ff. UrhG) schutzfähig.
Der Urheber hat das Recht zu bestimmen, ob und wie sein Werk zu veröffentlichen (§ 12 UrhG), ob das Recht mit einer **Urheberbezeichnung** zu versehen und welche Bezeichnung zu verwenden ist (§ 13 UrhG). Soweit Werke bereits in der Vergangenheit für andere Zwecke erworben wurden, muss überprüft werden, ob die Lizenzierung auch die Nutzung für eine Verbreitung über das Internet beinhaltet. Soweit sich aus dem Vertrag ergibt, dass das Internet nicht umfasst ist, muss eine Nachlizenzierung vorgenommen werden.

Weiterführende Literatur und Rechtsprechung:
Zum Zustimmungserfordernis bei Hyperlinks: *OLG Düsseldorf*, MMR 1999, S. 729; *LG Hamburg*, CR 2000, S. 776*; Ernst/Wiebe*, Immaterialgüterrechtliche Haftung für das Setzen von Links und vertragliche Gestaltungsmöglichkeiten, MMR Beilage 8/2001, S. 20ff. Allgemein zum Urheberrechtsschutz im Internet*: Hoeren/Sieber* (Hrsg.), Handbuch Multimedia- Recht, S. 77, Teil 7*; Hoeren*, Internetrecht, Stand: Oktober 2002, S. 72ff., abzurufen unter www.unimuenster.de/Jura.itm/hoeren/material/skript.pdf. Zum Urheberrechtsschutz von Datenbanken*: Milbradt*, Urheberrechtsschutz von Datenbanken, CR 2002, S. 710ff.

6.2 Was ist bei Kommunikationsangeboten zu beachten?

Kommunikationsangebote der Verwaltung sind im Folgenden solche auf Interaktion gerichteten Online-Angebote, die nicht den Erlass eines Verwaltungsaktes oder den Antrag eines Bürgers auf einen Verwaltungsakt zum Gegenstand haben. Primär wird also die allgemeine Online-Behördenkommunikation erfasst werden, die aufgrund ihrer Zweiseitigkeit über einseitige Online-Informationstätigkeit der Behörde hinausgeht. Wichtige Teile hiervon sind z.B. die einfache Kommunikation zwischen Bürger und Verwaltung mittels E-Mail (z.B. allgemeine Anfragen über Zuständigkeiten, Öffnungszeiten) sowie öffentliche Chat- und Diskussionsforen der Verwaltung. Sie können daher zwar Teil eines rechtsverbindlichen Online-Handelns im Rahmen eines Verwaltungsverfahrens gem. § 9 Verwaltungsverfahrensgesetz (VwVfG) sein (Auskunft über den Stand des laufenden Verfahrens), umfassen jedoch nicht den Antrag auf und Erlass von Verwaltungsakten. Diese Eckpunkte jedes Verwaltungsverfahrens werden vielmehr unter dem Stichwort der **Transaktionsangebote** behandelt (siehe unten S. 65). Soweit Regelungen des Verwaltungsverfahrens dabei beachtlich werden, wird das Bundes-VwVfG zugrunde gelegt. Denn dieses wurde bereits mit dem **Gesetz zur Anpassung des Verwaltungsverfahrensrechts an die moderne elektronische Kommunikation (3. VwVf-ÄndG)** an die Erfordernisse einer elektronischen Verwaltung angepasst. Von einer gleichartigen Änderung der Landes-VwVfG in naher Zukunft ist auszugehen. Typischerweise erfolgt die Kommunikation allerdings frei von Formvorschriften.

6.2.1 Was ist bei Kommunikation via E-Mail zu beachten?

Auch für die Kommunikation der Verwaltung mittels E-Mail besteht der Grundsatz der Formfreiheit, so wie er für das Verwaltungsverfahren ausdrückliche Berücksichtigung in § 10 VwVfG gefunden hat, hierüber hinaus aber auch als allgemeiner Rechtsgrundsatz Beachtung findet **(Vermutung der Formfreiheit).** Die Kommunikation mittels E-Mail ist daher zulässige Handlungsform der Verwaltung soweit keine abweichenden gesetzlichen Regelungen bestehen. Dies gilt sowohl für die Kommunikation zwischen Behörde und Bürger als auch für die Kommunikation zwischen Behörde und Behörde. Eine nähere Regelung der elektronischen Kommunikation erfolgte mit dem 3. VwVf-ÄndG.

Wann bestehen Vorschriften für die elektronische Verwaltungskommunikation, die vom Grundsatz der Formfreiheit abweichen?

Ausgangspunkt für Vorgaben der elektronischen Kommunikation bilden die Regelungen des neu in das VwVfG eingefügten § 3a. Die elektronische Kommunikation ist nur dann nicht möglich, wenn sie ausdrücklich oder implizit

ausgeschlossen ist. Dies ist etwa der Fall, wenn die persönliche Anwesenheit des Bürgers erforderlich ist (z.B. für Aushändigung und Entgegennahme einer Ernennungsurkunde, § 6 Abs. 2 BBG) oder sich das grundsätzliche Verfahrensermessen ausnahmsweise auf Null reduziert hat. Teilweise bestehen aber auch erhöhte Anforderungen an die elektronische Kommunikation, wenn besondere Rechtsvorschriften eine bestimmte Form des Verfahrens festlegen, insbesondere die Schriftform. Einem gesetzlichen Schriftformerfordernis im Verwaltungsverfahren kann nicht durch eine einfache E-Mail entsprochen werden; diese muss vielmehr gem. § 3a Abs. 2 VwVfG unter Einsatz einer qualifizierten elektronischen Signatur i.S.d. Signaturgesetzes erfolgen (hierzu unten S. 67). Auch untergesetzliche Regelungen wie z.B. Rechtsverordnungen können Schriftformerfordernisse enthalten.
Grundsätzlich gilt jedoch: liegen keine besonderen Formvorschriften vor, kann die Behörde innerhalb ihres pflichtgemäßen Ermessens auch via E-Mail kommunizieren.

Ist die Bürger-Einwilligung zur Online-Kommunikation notwendig?

Der Bürger muss gem. § 3a Abs. 1 VwVfG den Zugang für die Übermittlung elektronischer Dokumente eröffnet haben. Diese Form der Bürger-Einwilligung ist zwingende Voraussetzung für die Online-Kommunikation zwischen Bürger und Verwaltung. Das Merkmal der **„Zugangseröffnung"** beinhaltet hierbei zum einen als **objektives Element** das Vorliegen der technischen Voraussetzungen für eine elektronische Kommunikation, zum anderen als **subjektives Element** deren konkrete Nutzungsbestimmung durch den Bürger auch für eine Kommunikation mit der Verwaltung.

Wann liegt eine Einwilligung zur Online-Kommunikation vor?

Bei der Bestimmung der Zugangseröffnung sind die unterschiedlichen Ausgangssituationen von Bürger und Behörde zu beachten. Hierbei gilt, dass der **Bürger schützenswerter ist als die Behörde**, da der Bürger im überwiegenden Maße seine Internetverbindung für private E-Mail-Kommunikation nutzt. Die Verwaltung nutzt dagegen ihre Internetverbindung nur für dienstliche Zwecke.

- Daher kann bei der Angabe einer E-Mail-Adresse im Briefkopf des Bürgers nicht zwingend von seinem Willen ausgegangen werden, auch elektronisch mit der Behörde kommunizieren zu wollen. Anders als bei der Behörde kann sich ein privater Briefkopf auch nur an ein privates Umfeld richten. Wenn der Bürger selbst die Kommunikation mit der Verwaltung über das Internet aufnimmt, ist allerdings davon auszugehen, dass er auch den Zugang für eine E-Mail-Antwort eröffnet hat. Das elektronische Kommunizieren entspricht dann sogar dem in § 10 Abs. 2 VwVfG normierten Auftrag an die Verwaltung, das Verwaltungsverfahren einfach, zweckmäßig und zügig durchzuführen.
- Etwas anderes gilt dagegen für professionelle Anwender (Rechtsanwälte, Architekten). Ähnlich wie bei der Verwaltung steht hier die dienstliche Kommunikation im Vordergrund, so dass schon dann von einer Zugangseröffnung ausgegangen werden kann, wenn sich z.B. eine Angabe der E-Mail-Adresse auf dem Briefkopf befindet. Auch für die Frage des Zugangs von elektronischen Erklärungen wird diese Differenzierung relevant, vgl. hierzu S. 77.
- Entscheidend ist bei der Auslegung des Tatbestandsmerkmals der Zugangseröffnung letztlich auf die **Verkehrsanschauung** abzustellen. Das Tatbestandsmerkmal der Zugangseröffnung ist somit **entwicklungsoffen.**

Unter welchen Bedingungen ist die Verwaltung zur Online-Kommunikation verpflichtet?

Neben der Frage, wann die Behörde mittels Internet kommunizieren darf, stellt sich die Frage, ob für die Behörde in bestimmten Fällen auch eine rechtliche Verpflichtung zur Online-Kommunikation besteht. Wann muss also eine Behörde eine E-Mail zwingend als einen „Eingang" im verwaltungstechnischen Sinne bewerten und daher bearbeiten und wann muss sie ebenso auf elektronischem Wege antworten?
Ebenso wie auf Bürgerseite ist auch auf Verwaltungsseite zunächst eine Zugangseröffnung i.S.v. § 3a Abs. 1 VwVfG notwendig (vgl. oben). Dabei ergibt sich aus der Vorschrift des § 3a VwVfG **keine Pflicht der Behörde zur Zugangseröffnung**. Eine Verpflichtung der Verwaltung zur Online-Kommunikation besteht also zumindest solange nicht, wie keine Zugangseröffnung vorliegt.
Etwas anderes gilt jedoch dann, wenn generell durch die Behörde der Zugang zur elektronischen Kommunikation eröffnet wurde. Hier kann sich als Folge die **Pflicht der Behörde zur Annahme von E-Mails** ergeben,

- wenn die Behörde bereits mit einem Bürger via E-Mail kommuniziert und somit durch **vorangegangenes Tun** beim Bürger das Vertrauen erweckt hat, auch weiterhin den Verwaltungskontakt in dieser Sache mittels E-Mail abzuwickeln;
- wenn sich die Behörde mit einer **E-Mail Adresse auf Briefbögen oder Websites** präsentiert und hierdurch ihre Bereitschaft zur E-Mail Kommunikation signalisiert hat.
- Eine **Verpflichtung** der Behörde, elektronische Einträge auch **elektronisch zu beantworten**, besteht dagegen nur, soweit unter Berücksichtigung des Grundsatzes der Nichtförmlichkeit und des Auftrages an die Verwaltung, einfach, zweckmäßig und zügig zu handeln, die Nutzung der E-Mail Kommunikation für die Verwaltung bei Ausübung ihres pflichtgemäßen Ermessens geboten erscheint.

Aufgrund noch bestehender Unsicherheiten bei einer klaren Bestimmung der Zugangseröffnung wird der Verwaltung empfohlen, klarstellende Hinweise auf Umfang und Zulässigkeit der E-Mail-Kommunikation dort einzustellen, wo durch Angabe einer E-Mail-Adresse der Kommunikationsweg über das Internet zur Behörde eröffnet wird. Dies insbesondere dann, wenn der Umfang der elektronischen Kommunikation einer sachlichen Beschränkung unterliegen soll. Denn auch zu einer nur eingeschränkten Zugangseröffnung für bestimmte Verwaltungsdienste ist die Behörde gem. § 3a Abs. 1 VwVfG berechtigt ("*soweit*"). Zudem bietet es sich hierbei ebenfalls an, auf bestimmte Formatanforderungen und technische Rahmenbedingungen hinzuweisen (vgl. § 3a Abs. 3 VwVfG).

Kann die Verwaltung ausschließlich elektronische Verfahren anbieten?

Die Möglichkeit der Verwaltung, ausschließlich elektronische Verfahren anzubieten besteht nur, wenn die Verwaltung hierzu **ausdrücklich gesetzlich ermächtigt** wurde. Bereits eine Antragstellung im Verwaltungsverfahren, die das Benutzen und vollständige Ausfüllen bestimmter Formulare als Pflicht vorsieht, erfordert nach h.M. eine ausdrückliche gesetzliche Ermächtigung. Zur Zeit fehlt es der Verwaltung für ein ausschließlich elektronisches Verfahren an einer entsprechenden Ermächtigungsgrundlage. Die Vorschriften des VwVfG sehen die elektronische Kommunikation daher lediglich als **Alternative zu herkömmlichen Handlungsformen** vor. Dies ergibt sich bereits aus § 3a Abs. 1 VwVfG, welcher die elektronische Kommunikation nur zulässt, „*soweit*" die notwendigen technischen Voraussetzungen und zugleich auch der dahingehende individuelle Wille des Bürgers vorliegen. Eine Verpflichtung für den Bürger, die Voraussetzungen für eine elektronische Kommunikation zu schaffen, ergibt sich zumindest aus § 3a VwVfG nicht. Die elektronische Kommunikation ist daher z.Z. als **zusätzliche Option** zu verstehen.

Welche technischen Vorgaben darf die Verwaltung treffen?

Aus § 3a Abs. 3 S. 2 VwVfG folgt zumindest die implizite Ermächtigung der Verwaltung zur Festlegung von Standards wie z.B. Datenformaten etc., soweit dies für eine erfolgreiche elektronische Kommunikation unabdingbar ist. Denn die Behörde ist nach Gesetzeswortlaut verpflichtet, bei einer fehlerhaften Kommunikation "*die für sie geltenden technischen Rahmenbedingungen zu benennen*". Auch besteht für die Verwaltung zur Zeit noch die Möglichkeit, sich auf bestimmte Anbieter von elektronischen Signaturverfahren zu beschränken (hierzu unten S. 84).

Welche Folgen hat eine fehlgeschlagene elektronische Kommunikation für die Verwaltung?

§ 3a Abs. 3 VwVfG enthält Regelungen für den Fall der Übermittlung eines elektronischen Dokuments in einer für die Bearbeitung durch die Behörde oder den Bürger ungeeigneten Form. Im Rahmen des durch Aufnahme der Kommunikation geschaffenen **Verwaltungsrechtsverhältnisses** stellt § 3a Abs. 3 VwVfG an beide Seiten des Kommunikationsvorganges die Erwartung, dass sie die jeweils andere Seite bei fehlerhafter elektronischer Kommunikation hierüber informiert. Eine **ausdrückliche Pflicht zur Information trifft jedoch nur die Behörde**. Ist für diese ein übermitteltes elektronisches Dokument zur Bearbeitung nicht geeignet, muss sie dies dem Absender unverzüglich, also ohne **schuldhaftes Zögern** (§ 122 Abs. 1 S. 1 BGB) mitteilen. Hierbei hat sie dem Absender die geltenden technischen Anforderungen für eine Bearbeitung des elektronischen Dokuments (Datenformate u.ä.) zu nennen. Da in der Regel nur der Absender eine erneute Übermittlung desselben Dokuments in einem kompatiblen Format veranlassen kann, besteht die Informationspflicht nur ihm gegenüber.
Macht der Empfänger eines elektronisch übermittelten Behördendokuments dessen Ungeeignetheit zur Bearbei-

tung geltend, so trifft die Behörde ebenfalls die Pflicht, das Dokument erneut in einem **geeigneten elektronischen Format** oder als Schriftstück zu übermitteln. Regelungen über den Zugang elektronischer Dokumente soll § 3a Abs. 3 VwVfG dagegen nicht bereithalten. Dieser richtet sich vielmehr nach den allgemein hierzu entwickelten Grundsätzen des Verwaltungsverfahrensrechts (siehe zu Fragen des Zugangs elektronischer Erklärungen und Verwaltungsakte unten S. 77).

Besteht die Pflicht der Verwaltung zum Angebot und zur Nutzung von Verschlüsselungsverfahren?

Bei der Kommunikation mit dem Bürger fallen eine große Anzahl personenbezogener Daten sowohl der Behördenbeschäftigten als auch der Bürger an. Sie gilt es entsprechend den datenschutzrechtlichen Grundsätzen zu schützen. Bereits gem. § 30 VwVfG müssen die notwendigen Sicherheitsvorkehrungen getroffen werden, um einen Schutz von Geheimnissen im elektronischen Verwaltungsverfahren zu garantieren. Hierzu zählt auch die Verschlüsselung von Daten, sollen diese über das Internet übermittelt werden. Soweit es sich um Formen der Individualkommunikation handelt, können daneben die rechtlichen Anforderungen an die sicherheitstechnische Ausgestaltung für Teledienste des TDDSG Anwendung finden:

- Ist die Verwaltung als Teleddiensteanbieterin einzuordnen, hat sie gem. § 4 Abs. 4 Nr. 3 TDDSG durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer die Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. Das Angebot eines Teledienstes durch die Verwaltung besteht dann, wenn sie selbst eine Kommunikation über das Internet mittels ihrer Homepage bereithält. So z.B. bei der Möglichkeit, online Dokumente auszufüllen oder Anträge zu stellen.
- Für die Angebote der E-Mail-Kommunikation ist die Einordnung als Teledienst und damit das Erfordernis von Verschlüsselungsangeboten allerdings strittig. Die Bundes- und Landesdatenschutzbeauftragten gehen offenbar davon aus, dass das Angebot der E-Mail-Kommunikation als reines Angebot einer Telekommunikationsdienstleistung anzusehen ist. Dies hätte die Nichtanwendung des TDDSG und der sich hieraus ergebenen Pflichten zur Folge. Andere Stimmen ordnen gleichwohl auch E-Mail-Angebote als Teledienst ein und verlangen von der Verwaltung grundsätzlich entsprechende Vorkehrungen, wenn sie einen eigenen E-Mail-Service mittels eines eigenen Providers anbietet.

Unabhängig von der Reichweite der Verpflichtungen des TDDSG wird aber der Verwaltung empfohlen, jedenfalls für die E-Mail-Kommunikation mit ihren Angeboten, Verschlüsselungsverfahren bereit zu stellen. Hierdurch wird eine sichere Abwicklung und ein datenschutzgerechtes Diensteangebot gewährleistet. Der Bürger ist allerdings zumindest hinsichtlich seiner eigenen Daten grundsätzlich nicht verpflichtet, die durch die Verwaltung angebotenen Verschlüsselungsmöglichkeiten auch zu nutzen.
Die Verwaltung ist aufgrund datenschutzrechtlicher Vorgaben dagegen verpflichtet, bei der Übermittlung via E-Mail personenbezogene oder andere schutzbedürftige Daten zu verschlüsseln. Zu den verschiedenen technischen Möglichkeiten der Umsetzung dieser Fragen siehe näher die Handlungsempfehlungen der Bundes- und Landesdatenschutzbeauftragten, Datenschutzgerechtes eGovernment, Dezember 2002, S. 38.

Welche Anforderungen bestehen bei E-Mail-Kommunikation für die Aktenführung?

Auch bei einer elektronischen Kommunikation der Verwaltung bleibt die sich aus § 29 VwVfG mittelbar ergebende Verpflichtung zum Führen von Akten bestehen. Dies folgt aus dem umfassenden Aktenbegriff des VwVfG, welcher auch Datenträger sowie Dateien einschließlich der zu ihrer Auswertung erforderlichen Programme erfasst (materieller Aktenbegriff). Ein vergleichbares Aktenverständnis besteht in den jeweiligen Archivgesetzen (ArchivG) der Länder und des Bundes. Ein behördliches Bedürfnis der sicheren Aktenführung bzw. Archivierung ergibt sich darüber hinaus auch aus Gründen der Beweissicherung.
Das **Gebot der Aktenmäßigkeit** beinhaltet ein **Gebot der Vollständigkeit** einschließlich **des Gebots der Führung wahrheitsgetreuer Akten.** Deshalb muss grundsätzlich auch die das Verwaltungsverfahren betreffende E-Mail-Kommunikation aus Verfahrensakten ersichtlich werden. Ob dies jede E-Mail betrifft, die innerhalb eines Verwaltungsverfahrens ausgetauscht wird, ist jedoch unklar. Es besteht der Grundsatz, dass schriftliche Äußerungen in aller Regel zu den Akten zu nehmen sind, Telefonate und andere Formen des informellen Handelns je nach Bedeutung für das Verwaltungsverfahren. Ob eine E-Mail eher als informelles Handeln oder schriftliche Äußerung zu werten ist, wird daher im Einzelfall zu prüfen und hieran die Entscheidung

zur Aufbewahrung zu koppeln sein. Erfolgt erst im Einzelfall die Kommunikation elektronisch, ansonsten aber noch in Papierform, so sind zusätzliche Anforderungen hinsichtlich sog. hybrider Akten zu berücksichtigen. Vgl. hierzu und zur elektronischen Aktenführung im Verwaltungsverfahren unten S. 79.

Welche Regelungsaspekte sollen von einer Dienstanweisung über die Nutzung von E-Mail Systemen am Arbeitsplatz umfasst werden?

Um **verwaltungsinterne Standards** für die E-Mail Kommunikation zu setzen, bietet sich der Erlass von Dienstanweisungen zur Benutzung und Behandlung elektronischer Post an. Bei der Erstellung sollte die Personalvertretung eingebunden werden. Für eine vertiefende Darstellung wird insbesondere auf die Musterdienstanweisung der Arbeitsgruppe *"DA elektronische Post"* des Bayerischen Städtetags verwiesen. Folgende Regelungsaspekte sollten aber unbedingt von einer Dienstanweisung umfasst werden:

- Die **private Nutzung der elektronischen Post/des Internet** kann grundsätzlich verboten werden. Hierdurch wird vermieden, dass Träger der Verwaltung als Telediensteanbieter im Sinne des TDG eingestuft werden könnten; eine Anwendung der erhöhten Anforderungen des TDDSG für Telediensteanbieter wird hierdurch vermieden. Ein solches Verbot steht in der Praxis einer Duldung der privaten Nutzung nicht entgegen.
- Für die **Einrichtung von Postfächern** sollte durch Dienstanweisung geregelt werden, welche Organisationseinheit der Verwaltung ein zentrales Postfach zugewiesen bekommt. Auch sollte für die Postfächer der Bediensteten sowie der Organisationseinheiten ein einheitliches Schema der Adressenvergabe gefunden werden, welches es ermöglicht, durch logische Verknüpfung die E-Mail-Adresse zu erstellen (z.B. nachname@stadtname.de)
- Die **Regelung des Posteingangs** sollte eine regelmäßige Posteingangskontrolle vorschreiben, Regelungen bei Abwesenheit (Urlaub/Krankheit) sowie Regelungen für falsch adressierte Post treffen und schließlich eine Virenprüfung vorschreiben. Auch sollte eine Regelung getroffen werden, die den Grundsätzen einer ordnungsgemäßen Aktenführung entspricht.
- Eine dienstliche Anweisung zur **Regelung des Postausgangs** sollte für die Übermittlung sensibler Daten mittels E-Mail zur Nutzung geeigneter Verschlüsselungsverfahren verpflichten. Die Regelung zur Gestaltung der E-Mail sollte sich an Behördenkommunikation in Papierform anlehnen, also deutlich den Betreff der E-Mail, den Absender und die absendende Behörde bzw. Dienststelle erkennen lassen.
- Eine Dienstanweisung sollte letztlich sowohl für den Posteingang als auch für den Postausgang Regelungen treffen, die auch für diese Bereiche die **Grundsätze einer ordnungsgemäßen Aktenführung** berücksichtigen.

Weiterführende Literatur:
Zu grds. Fragen der Verwaltungskommunikation via E-Mail: *Roßnagel*, Das elektronische Verwaltungsverfahren, NJW 2003, S. 469 ff.; *Ries* in: Kröger (Hrsg.), Internetstrategien für Kommunen, Köln 2001; Siehe als Beispiel einer Dienstanweisung für die elektronische Kommunikation den Musterentwurf einer Dienstanweisung zur Benutzung und Behandlung elektronischer Post "DA elektronische Post" des Bayerischen Städtetags, Stand 1999. Zu Verschlüsselungsangeboten durch die Verwaltung: LfD Niedersachsen *Nedden* (Hrsg.), Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung, Hannover 2001, S. 25ff. Zu Sicherheitskonzepten der E-Mail-Kommunikation: *Bertsch/Stark*, Verschlüsselung und Inhaltssicherung, DuD 25 (2002), S. 711ff. Zu Fragen der Archivierung bei E-Mail-Kommunikation: *Britz*, Reaktion des Verwaltungsverfahrensrechts auf die informationstechnische Vernetzung der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsverfahren und Verwaltungsverfahrensgesetz, Baden-Baden 2002, S. 213 (257ff.).

6.2.2 Was ist bei der Veranstaltung von öffentlichen Diskussionsforen durch die Verwaltung zu beachten?

Neben der individuellen Kommunikation via E-Mail rücken verstärkt Kommunikationsangebote der Verwaltung in den Vordergrund, die sich in Form von Diskussions- und Chatforen an die breite Öffentlichkeit wenden („**Marktplatz der Meinungen**"). Hierbei richten sich die allgemeinen Pflichten für ein solches Angebot erneut nach ihrer medienrechtlichen Einordnung (vgl. S. 42). Daneben ist die Formulierung von Verfahrensregelungen und Nutzungsbedingungen beachtlich. Dies zum einen um die notwendige Transparenz und Objektivität staatlicher Diskussionsforen zu gewährleisten, zum anderen, um über eine Rechtsgrundlage für das Vorgehen gegen Störer des öffentlichen Angebots zu verfügen. Letztlich kann auch eine organisatorische Auslagerung sinnvoll sein (z.B. eingetragener Verein als Veranstalter).

Wie sind öffentliche Diskussionsforen rechtlich einzuordnen?

Auch für Chat- und Diskussionsforen ergibt sich keine eindeutige Einordnung in die Regelungsstruktur der relevanten Gesetze. Teile der Literatur ordnen Chat-Foren (Internet-Relay-Chat, aber auch offene Mailinglisten und Newsgroups) als Mediendienst i.S.v. § 2 Abs. 2 Nr. 4 MDStV ein. Andere Teile der Literatur ordnen **unmoderierte Diskussionsforen** als Teledienst ein, verweisen jedoch zugleich darauf, dass ebenso die Möglichkeit zur Einordnung als Mediendienst bestünde und daher die Kollisionsnorm des § 2 Abs. 4 Nr. 3 TDG Anwendung finden soll. Hieraus soll sich dann ergeben, dass zumindest unmoderierte Newsgroups und Diskussionsforen als Teledienste nach § 2 Abs. 2 Nr. 2 TDG einzuordnen seien. Eine andere Einordnung soll jedoch für **moderierte Diskussionsforen** möglich sein, da hier das in § 2 Abs. 3 Nr. 4 TDG zur Abgrenzung von TDG / MDStV genannte Merkmal der "redaktionellen Gestaltung" eine stärkere Gewichtung erhalten könnte. Entscheidend wäre dabei, ob der Moderator selbst Einfluss auf die Präsentation der Nachrichten oder ihre Gruppierung nimmt.

Im Ergebnis ist somit die noch immer bestehende **Unsicherheit bei Einordnung** von Chat- bzw. Diskussionsforen festzuhalten. Es bietet sich daher aus praktischen Erwägungen an, Vorschriften des MDStV und des TDG **gleichermaßen zu berücksichtigen**. Dies stellt aufgrund weitreichender inhaltlicher Überschneidungen beider Gesetze keine zu hohen Anforderungen. Denn unabhängig von der Einordnung als Medien- oder Teledienst sind die Pflichten auf Seiten der Verwaltung bei Angebot eines moderierten öffentlichen Diskussions- und Partizipationsforums für Bürger aus TDG, TDDSG oder MDStV nahezu identisch. Vgl. zu den allgemeinen Pflichten eines Diensteanbieters oben unter 5.

Besondere Anforderungen treten für den Anbieter eines Gästebuchs oder eines Diskussionsforums mit Archivfunktion allerdings im Bereich der Haftung für Inhalte auf. Grundsätzlich kann sich der Anbieter eines Chatforums o.ä. auf die **Haftungsprivilegierung** der §§ 6ff. MDStV bzw. der §§ 8ff. TDG für fremde Inhalte berufen. Dies gilt jedoch dann nicht, wenn der Anbieter (auch die Verwaltung) sich fremde Inhalte durch deren Duldung zu Eigen macht. Dann muss sich der Anbieter auch für solche Inhalte verantworten. Für die Verwaltung als Diensteanbieter besteht daher die Verpflichtung, Einträge in **Gästebücher** etc. **regelmäßig zu kontrollieren** und rechtsverletzende Inhalte zu löschen. Auch ein distanzierender Hinweis in Nutzungsbedingungen oder ähnlichem kann dies nicht verhindern. In welchen zeitlichen Abständen eine Kontrolle zu erfolgen hat, soll nach der Rspr. von den Umständen des Einzelfalls abhängen. Vgl. zu Fragen der Haftung für Inhalte allgemein oben S. 43.

Wann sind Nutzungsbedingungen sinnvoll?

Eine Formulierung von expliziten Nutzungsbedingungen für die Teilnahme an durch die öffentliche Hand bereitgestellten Chat- und Diskussionsforen bietet sich aus mehreren Gründen an. Zunächst kann zusammen mit der Formulierung der Nutzungsbedingungen allgemein auf die Funktion und Zielrichtung eines solchen Angebots eingegangen werden. Hierdurch kann grundsätzlichen Anforderungen wie **Publizität und Nachvollziehbarkeit** des staatlichen Handelns entsprochen werden. Weiter sind Nutzungsbedingungen jedoch auch für das konkrete Verhältnis zwischen einzelnem Nutzer und anbietender Verwaltung wesentlich. Der Verwaltung wird eine **rechtliche Grundlage** geboten, **gegen Teilnehmer vorzugehen**, wenn diese gegen die in den Nutzungsbedingungen formulierten Grundsätze verstoßen. Denn nimmt ein Dritter das Angebot der Behörde zur Teilnahme an Chat- und Diskussionsforen war, so akzeptiert er zugleich die hierfür aufgestellten Nutzungsbedingungen. Diese können neben dem Ausschluss eines Nutzers auch die Sperrung oder Löschung von Inhalten und Accounts umfassen. Es ist hierbei zulässig, bestimmte Umgangsformen u.ä. zum Schutze Dritter aber auch zum Schutz der Freiheit der sich Äußernden zu definieren. Ein bloßer Verweis auf die in Internet-Foren übliche Netiquette ist hierbei nicht ausreichend.

Welche Regelungsaspekte sollen von einer Nutzungsbedingung umfasst werden?

Durch die ausdrückliche Formulierung von **Nutzungsbedingungen** kann auch solches Verhalten sanktioniert werden, welches noch nicht durch allgemeine Vorschriften z.B. des Strafrechts erfasst ist. Zugleich bedeutet dies aber auch, dass die **Verwaltung ebenfalls an die formulierten Grundsätze gebunden** ist. Ohne eine konkrete Verletzung der Nutzungsbedingungen wird der Ausschluss eines einzelnen Nutzers daher kaum zu rechtfertigen sein. Sinnvoll erscheint es in diesem Zusammenhang auch**, zur Akzeptanzbildung eine Schlichtungsstelle** für ein Schlichtungs-

verfahren in Streitfällen zu benennen (verfahrensmäßige Verhältnismäßigkeit). Aus den genannten Gründen sollte bei einer Formulierung von Nutzungsbedingungen daher insbesondere berücksichtigt werden, dass:

- die Nutzungsbedingungen für die Teilnahme an einem öffentlichen Forum die **Transparenz des Angebots** gewährleisten und inhaltliche Steuerungen des Diensteanbieters für den Teilnehmer **nachvollziehbar** ablaufen;
- durch die Formulierung von objektiven Kriterien die willkürliche oder einseitig interessengesteuerte Meinungsbeschränkung unterbunden wird;
- **deutliche Formulierungen die Nutzungsformen** darlegen und **untersagte Handlungsformen** ausdrücklich benennen. Hierbei ist es nicht erforderlich, bereits durch gesetzliche Vorschriften (StGB usw.) verbindliche Verbote erneut zu benennen, teilweise kann dies jedoch von beiderseitigem Interesse sein;
- die Folgenseite (mögliche Sanktionen) der Nutzungsbedingungen so formuliert werden, dass dem Nutzer die Konsequenzen eines Verstoßes bewusst sind und die Verwaltung über eine **klare Grundlage für ein Einschreiten gegenüber Störern** ihres Angebotes verfügt;
- Regelungen einer Nutzungsordnung und eine Einwilligung des Nutzers nicht die **individuelle Einwilligung** in die Verarbeitung personenbezogener Daten ersetzen können, wenn diese nach den einschlägigen Gesetzen erforderlich ist;
- ausdrücklich auf die **Möglichkeit einer Sperrung bzw. einer Löschung von Beiträgen** bei Verstoß gegen die Nutzungsbedingungen hingewiesen wird.
- Zu der Frage einer wirksamen Einbeziehung der Nutzungsbedingungen in das Diensteverhältnis siehe oben unter allgemeine Anbieterpflichten S. 45.

Können „störende" Teilnehmer von öffentlichen Angeboten ausgeschlossen werden?

Auch für solche Fälle, in denen keine ausdrücklichen Nutzungsbedingungen durch den Veranstalter von Chat- und Diskussionsforen vorliegen, wurde durch die Rechtsprechung dem Service-Provider die Möglichkeit zugestanden, "störende" Teilnehmer von der Nutzung des Internet-Angebots auszuschließen. Das Landgericht Bonn hatte hierbei eine mögliche Rechtsgrundlage für den Ausschluss in § 1004 BGB gesehen und dem Service-Provider ein "virtuelles Hausrecht" an seinem Chat-Angebot zugestanden. Hieraus ergeben sich nach Rspr. des LG Bonn ähnliche Rechte, wie sie das Zivilrecht für das Eigentum vorsieht. Zu beachten ist jedoch, dass auch bei der Annahme eines „**virtuellen Hausrechts**" kein beliebiges Recht zum Ausschluss einer einzelner Nutzer besteht, wenn zuvor das Chat-Angebot allgemein an die Öffentlichkeit gerichtet gewesen ist. Denn der Diensteanbieter hat mit seinem generellen Angebot und einer Eröffnung des Zugangs zum Chat-Forum zunächst die Einwilligung zur Nutzung seines "virtuellen Eigentums" gegeben, für den Widerruf dieser Einwilligung müssen nun besondere Gründe vorliegen. Aus dem **„Verbot des widersprüchlichen Verhaltens**" (§ 242 BGB) ergibt sich, dass ein Ausschluss ohne sachlicher Rechtfertigung unzulässig ist. Insgesamt ist die Konstruktion eines "virtuellen Hausrechts" jedoch noch neu und erst teilweise von der Rspr. anerkannt. Die Angebote der Verwaltung sollten daher gründlich formulierte Nutzungsbedingungen aufweisen, um rechtliche Hilfskonstruktionen für die Begründung der Sperrung einzelner Teilnehmer oder die Löschung einzelner Beiträge zu vermeiden.

Weiterführende Literatur und Rechtsprechung:
Ladeur, Verfassungsrechtliche Fragen regierungsamtlicher Öffentlichkeitsarbeit und öffentlicher Wirtschaftstätigkeit im Internet, DÖV 2002, S. 1 ff. Zur Haftung für Äußerungen in einem Internet-Gästebuch: *LG Düsseldorf,* Urt. v. 14.08.2002, Akz.: 2 a O 312/01, JurPC Web-Dok. 323/2002. Zu den datenschutzrechtlichen Vorgaben für das Betreiben eines Chat-Forums*: Schaar/Schulz,* in Roßnagel (Hrsg.), Recht der Multimedia-Dienste, Loseblatt-Kommentar , § 4 TDDSG Rnr. 44ff. Siehe als Formulierungsbeispiel einer Nutzungsbedingung bzw. Haftungsausschlüsse die Nutzungsbedingung des Esslinger Bürgerforum unter http://forum.esslingen.de. Zu Fragen inhaltlicher Regulierung staatlicher Chat- und Diskussionsforen: *LG Bonn*, Urt. v. 16.11.1999, NJW 2000, S. 961; LG Potsdam, CR 2000, S. 123. Zu Fragen der Haftung für Inhalte*: OLG München*, MMR 2002, S. 611 (Gewerbeschädigende Äußerungen in einem Meinungsforum im Internet); *AG Charlottenburg*, JurPC Web-Dok. 336/2002 (Persönlichkeitsrechtsverletzung durch Text in einer Newsgroup); *Ladeur*, Ausschluss von Teilnehmern an Diskussionsforen im Internet, MMR 12/2001, S. 787ff. Zu Fragen der technischen Kontrollmöglichkeiten von Chat-Foren, insb. unter dem Einsatz von Filtersoftware: *Sieber*, Verantwortlichkeit im Internet, München 1999, S. 43ff.

6.3 Was ist für Transaktionsangebote zu berücksichtigen?

Unter dem Begriff der Transaktion werden im Folgenden alle Formen des rechtsverbindlichen elektronischen Verwaltungshandelns verstanden. Im Vordergrund stehen hierbei solche Formen des Verwaltungshandelns, die bestimmte Formerfordernisse erfüllen müssen und daher an eine elektronische Abwicklung im Vergleich zur Information und Kommunikation erhöhte Anforderungen stellen.

6.3.1 Unter welchen Voraussetzungen kann zwischen Bürger und Verwaltung eine rechtsverbindliche Online-Transaktion stattfinden?

Grundsätzlich ist auch die rechtsverbindliche Online-Transaktion formlos möglich. Allerdings können sich für die öffentliche Verwaltung insbesondere aus dem VwVfG, Spezialgesetzen aber auch aus Verwaltungsvorschriften, Verwaltungsvereinbarungen und Dienstanweisungen Formerfordernisse für ein elektronisches Verwaltungshandeln ergeben.

Gem. § 3a Abs. 2 VwVfG ist im Falle eines gesetzlich angeordneten Schriftformerfordernisses im Regelfall die elektronische Kommunikation unter Verwendung einer qualifizierten elektronischen Signatur zulässig. § 3a Abs. 2 VwVfG regelt die elektronische Kommunikation in Form einer **Generalklausel**. Sie gilt für alle Schriftformerfordernisse im Verwaltungsverfahren, es sei denn, dass der Gesetzgeber **ausdrückliche Ausnahmen** hiervon normiert hat. Daher können für die Verwaltung die Anforderungen an eine rechtsverbindliche Online-Transaktion teilweise auch höher liegen. So kann gem. § 37 Abs. 4 VwVfG für einen Verwaltungsakt durch Rechtsvorschrift die **dauerhafte Überprüfbarkeit** der elektronischen Signatur vorgeschrieben werden, welche zur Zeit nur durch qualifizierte elektronische Signaturen eines akkreditierten Zertifizierungsdiensteanbieters gewährleistet wird. Es können ebenfalls Abweichungen vom Sicherheitsniveau der qualifizierten elektronischen Signatur nach "unten" vorgenommen werden. Teilweise wird die elektronische Kommunikation auch völlig ausgeschlossen. Abweichungen von der Generalklausel des § 3a Abs. 2 VwVfG werden im Gesetzestext folgendermaßen zum Ausdruck gebracht:

- Das Begriffspaar „**schriftlich oder elektronisch**" wird vom Gesetzgeber verwendet, wenn bei gesetzlich angeordneter Schriftform auch einfache Formen elektronischer Kommunikation ausreichen sollen. Eine qualifizierte elektronische Signatur ist hier nicht erforderlich.
- Soll die Generalklausel des § 3a Abs. 2 VwVfG überhaupt keine Anwendung finden und auch keine sonstige Form der elektronischen Kommunikation erfolgen, wird dies vom Gesetzgeber explizit mit den Formulierungen "**die elektronische Form ist ausgeschlossen**" / "**§ 3a VwVfG findet keine Anwendung**" zum Ausdruck gebracht.

Weiterführende Literatur:
Zum 3. VwVf-ÄndG: *Britz*, Reaktion des Verwaltungsverfahrensrechts auf die informationstechnische Vernetzung der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsverfahren und Verwaltungsverfahrensgesetz, Baden-Baden 2002, S. 213ff.; *Catrein*, Anmerkungen zum Entwurf eines Gesetzes zur Änderung der Verwaltungsverfahrensgesetze des Bundes und der Länder, NVwZ 2001, S. 413ff.; *Schmitz/Schlatmann*, Digitale Verwaltung? Das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften, NVwZ 2002, S. 1281ff.

6.3.2 Wie funktioniert die qualifizierte elektronische Signatur?

Bei der qualifizierten elektronischen Signatur wird durch Verwendung eines **privaten kryptographischen Schlüssels** „signiert". Diesem steht ein **öffentlich zugänglicher Schlüssel** zur Überprüfung der Signatur gegenüber. Die verwendeten Schlüssel sind einmalig und einer natürlichen Person fest zugeordnet. Der private Schlüssel ist geheim zu halten und kann nur in Verbindung mit einer PIN oder einem ähnlich sicheren biometrischen Merkmal zum Signieren verwendet werden. Ein beglaubigtes Signaturschlüssel-Zertifikat ordnet dem Signaturschlüssel-Inhaber den öffentlichen Schlüssel zu. Ausgestellt wird das qualifizierte Zertifikat von einem Zertifizierungsdiensteanbieter als „vertrauenswürdigem Dritten". Dieser hält das Zertifikat (mit dem öffentlichen Schlüssel) nach § 5 Abs. 1 SigG – je nach Wunsch des Schlüsselinhabers – nachprüfbar oder abrufbar.

Um für den Signaturvorgang eine zeitaufwendige vollständige Verschlüsselung des gesamten Dokuments zu vermeiden, wird i.d.R. nicht das Dokument, sondern ein sog. **Hash-Wert** mit dem privaten Schlüssel signiert. Bei einem Hash-Wert handelt es sich um eine mathematische Reduktion der zu signierenden Daten beliebiger Länge auf einen Wert fester Länge (sog. **Algorithmen**), welche den einzigartigen „Fingerabdrucks" des Gesamtdokuments bildet. Dieser Hash-Wert wird verschlüsselt. Dieses **Kryptogramm** ist die elektronische Signatur. Der Empfänger eines elektronisch signierten Dokuments erhält also zum einen das Dokument in seiner ursprünglichen Form und zusätzlich in Form der Signatur eine Art „mathematischen Fingerabdruck". Nach Empfang werden zur Überprüfung der Unversehrtheit nun erneut zwei Hash-Werte gebildet. Eines nach dem normalen Verfahren aus dem übersendeten Dokument und einer durch Rücktransformation der Signatur mit Hilfe des öffentlichen Schlüssels in den ursprünglichen Hash-Wert. Stimmen beide Werte überein, so bedeutet dies, dass der übersendete Text während des Übermittlungsvorgangs nicht

verändert wurde. Die elektronische Signatur gibt dann im Ergebnis verbindlich Auskunft über den Absender und Unterzeichner des Dokuments. Eine qualifizierte elektronische Signatur garantiert also insbesondere die sichere **Authentifizierung** des Kommunikationspartners mittels gesendeten Zertifikats und dessen Gültigkeit sowie die Überprüfung der **Integrität** der übermittelten Daten mittels Abgleichung der Hash-Werte. Hierdurch entsteht eine **Funktionsäquivalenz** der elektronischen zur handschriftlichen Signatur:

- Die **Echtheitsfunktion** einer Signatur gewährleistet, dass eine Erklärung wirklich vom Unterzeichner stammt. Auf elektronischem Wege wird diese Funktion durch mathematisch-logische Verbindung von Text und Signatur erbracht.
- Die **Identitätsfunktion** wird zur Identifikation des Autors eines Dokuments genutzt. Bei Verwendung der klassischen Papierform wurde die Identität aufgrund der Einzigartigkeit der Hand- bzw. Unterschrift ermittelt. Eine qualifizierte elektronische Signatur erfüllt diese Funktion mittels der Einmaligkeit des nur einer einzigen Person zugeordneten privaten Schlüssels und des Nachweises dieser Zuordnung in einem Zertifikat des Diensteanbieters. Das erreichte Sicherheitsniveau dürfe das einer handschriftlichen Unterschrift übertreffen. Zur Problematik der sog. Namensgleichheit siehe S. 85.
- Auch die **Garantiefunktion** dient ebenso wie Echtheits- und Identitätsfunktion der Authentizität eines Dokuments. Sie bietet die Möglichkeit, einzelne Merkmale der Unterschrift mit bereits vorhandenen Unterschriften desselben Unterzeichners zu überprüfen. Gerade eine elektronische Signatur ermöglicht die Überprüfung der Echtheit eines elektronischen Dokuments und (im begrenzten Umfang) der Identität seines Erstellers.
- Die **Perpetuierungsfunktion** erfordert eine feste Verkörperung von Erklärungen etc., um die Integrität ihrer Inhalte zu sichern und eine dauerhafte Lesbarkeit zu ermöglichen. Elektronische Dokumente stellen gerade keine solche Verkörperung dar, denn ohne dass es für den Betrachter zu erkennen wäre, können sie vielfach manipuliert werden. Die Verwendung einer elektronischen Signatur schützt jedoch das Textdokument vor Veränderungen bzw. lässt solche auch für Dritte erkennbar werden, so dass der Perpetuierungsfunktion auch ohne Verkörperung entsprochen wird.
- Die **Abschlussfunktion** dient der Abgrenzung einer willentlichen und rechtsverbindlichen Erklärung von bloßen Vorschlägen und Entwürfen. Bei Verwendung einer elektronischen Signatur wird dem bereits mit dem Umstand entsprochen, dass auch hier der Erklärende in der Regel seine elektronische Erklärung nach Abschluss einer "Überlegungsphase" signieren wird und über die rechtliche Erheblichkeit seiner Erklärung informiert wurde.
- Die **Warnfunktion** einer Unterschrift dient dazu, den Unterzeichnenden über die Rechtsverbindlichkeit seines Handelns aufzuklären. An eine stoffliche Form der Unterzeichnung ist sie nicht gebunden. So kann der Warnfunktion auch elektronisch entsprochen werden, wobei die tatsächliche Wirkung stark von dem individuellen Verständnis des Einzelnen für die neuartige Form der elektronischen Signatur abhängen dürfte. Die Warnfunktion spielt allerdings im Verwaltungsrecht nur eine untergeordnete Rolle.

6.3.3 Welche Signaturen für die Verwaltung? – Die unterschiedlichen Regelungsniveaus

Gem. § 2 Nr. 1 SigG sind elektronische Signaturen alle Daten, die anderen elektronischen Daten beigefügt werden und zur **Authentifizierung** dienen. Das SigG definiert somit alle Formen der elektronischen Signatur, selbst Signaturen ohne Sicherheitswert (so z.B. auch eingescannte Unterschriften). Hierbei unterscheidet das SigG allerdings zwischen drei unterschiedlichen Sicherheitsniveaus für elektronische Signaturen: die einfachen oder sonstigen elektronischen Signaturen, qualifizierte elektronische Signaturen i.S.v. § 2 Nr. 3 SigG und qualifizierte elektronische Signaturen eines akkreditierten Zertifizierungsdiensteanbieters gem. § 2 Nr. 3 i.V.m. § 15 SigG (im Folgenden akkreditierte Signatur). Für das rechtskonforme Handeln in elektronischer Form sind für die Verwaltung nur die beiden letztgenannten Signaturen bedeutsam und nur für diese Signaturverfahren enthält das SigG auch materielle Anforderungen:

- **Qualifizierte elektronische Signaturen** müssen gem. § 2 Nr. 3 a SigG auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und gem. § 2 Nr. 3 b mit einer sicheren Signaturerstellungseinheit erzeugt sein. An sie richten sich die Erfordernisse der §§ 5-14 SigG. Hier werden die Vergabe von qualifizierten Zertifikaten, ihr Inhalt und die sich

hieraus ergebenen Pflichten für den Zertifizierungsdienstebetreiber geregelt. Der Zertifizierungsdiensteanbieter muss für das Angebot qualifizierter Zertifikate seinen Betrieb nur **anzeigen** und **glaubhaft darlegen**, dass er die Anforderungen des SigG erfüllt.

- **Akkreditierte Signaturen** sind qualifizierte elektronische Signaturen i.S.v. § 2 Nr. 3 a SigG, deren Zertifikat durch einen Diensteanbieter ausgestellt wurde, der die Erfordernisse der §§ 5-14 SigG erfüllt und dieses zusätzlich in einer **Vorabprüfung (freiwillige Akkreditierung**) i.S.v. § 15 SigG nachgewiesen hat. Qualifizierte elektronische Signaturen eines akkreditierten Zertifizierungsdiensteanbieters bieten daher das höchste Sicherheitsniveau des SigG. Nur bei Ihnen ist amtlich geprüft und bestätigt, dass der Anbieter alle gesetzlichen Anforderungen erfüllt hat. Dagegen verfügen die Verfahren zur Erstellung einer qualifizierten elektronischen Signatur lediglich über eine glaubhaft gemachte, nicht jedoch geprüfte und nachgewiesene Infrastruktur.

Eine differenzierte Darstellung der Unterschiede zwischen den beiden Signaturen findet sich in der nachfolgenden Tabelle.

Abbildung 5: Signaturen und ihre rechtlichen Unterschiede im Überblick

	″akkreditierte Signatur″	″qualifizierte Signatur″
Schriftformersatz	§ 126a BGB, § 3a VwVfG: Ersatz für gesetzlich vorgeschriebene Schriftform. Auch Schriftformersatz, soweit für die Signatur die dauerhafte Überprüfbarkeit vorgeschrieben ist: grundsätzlich möglich für Verwaltungsakte (VA) (§ 37 Abs. 4 VwVfG); bisher vorgesehen z.B. für VA für Abschluss des förmlichen Verwaltungsverfahrens (§ 69 Abs. 2 S. 2 VwVfG) und für Unterschrift des Bediensteten bei Beglaubigungsvermerk (§ 33 Abs. 5 Nr. 2 VwVfG).	§ 126a BGB, § 3a VwVfG: Ersatz für gesetzlich vorgeschriebene Schriftform. Risiko des Nicht-Bestehens der behaupteten Sicherheit. Grundsätzlich kein Schriftformersatz, soweit für die Signatur die dauerhafte Überprüfbarkeit vorgeschrieben ist
Beweiseignung	§ 292a ZPO: Anschein der Echtheit der Signatur. Für Nachweis qualifizierter Signatur: Inanspruchnahme der ″technisch-organisatorischen″ Sicherheitsvermutung nach § 15 Abs. 1, Abs. 4 SigG.	§ 292a ZPO: Anschein der Echtheit der Signatur. Für Nachweis qualifizierter Signatur: Allenfalls Bitte an den Richter möglich, vom Signaturaussteller die Vorlage der Signaturerstellungseinheit (§ 144 ZPO) und vom Zertifizierungsdiensteanbieter die Vorlage seiner Dokumentation (§ 142 ZPO) zu verlangen.
Nachweis organisatorischer Sicherheit	§ 15 Abs. 1 S. 4 SigG: ″Nachweis umfassend geprüfter administrativer Sicherheit″. § 15 Abs. 1 S. 3 SigG: Gütezeichen der RegTP.	Anzeigepflicht mit Darlegung, dass Voraussetzungen nach § 4 Abs. 3 SigG vorliegen. Keine vorherige Überprüfung der Voraussetzungen.
Nachweis technischer Sicherheit	§ 15 Abs. 1 S. 4 SigG: ″Nachweis umfassend geprüfter technischer Sicherheit″. § 15 Abs. 7 SigG: Vorabüberprüfung aller technischen Komponenten für den Einsatz in akkreditierten Signaturverfahren nach dem Stand von Wissenschaft und Technik und nach den Vorgaben des Abschnittes I der Anlage 1 SigV (vgl. § 11 Abs. 3 SigV).	§ 17 Abs. 4 SigG: Vorabüberprüfung nur für die sichere Signaturerstellungseinheit und die Komponenten der Schlüsselerzeugung nach den Verfahren des Abschnitts II der Anlage 1 SigV (§ 15 Abs. 5 S. 2 SigV) und entsprechende Anwendung der Anforderungen nach Abschnitt I ohne Verweis auf den Stand von Wissenschaft und Technik.

	"akkreditierte Signatur"	"qualifizierte Signatur"
Langzeitprüfbarkeit bei fortlaufendem Betrieb	§ 4 Abs. 2 SigV: Zertifikate müssen mindestens 30 Jahre ab dem Schluss des Jahres, in dem ihre Gültigkeit endet, prüfbar und abrufbar gehalten werden.	§ 4 Abs. 1 SigV: Zertifikate müssen für die Dauer ihrer Gültigkeit plus 5 Jahre ab Jahresende aufbewahrt und prüfbar oder abrufbar gehalten werden.
Langfristdokumentation bei fortlaufendem Betrieb	§ 8 Abs. 3 i.V.m. § 4 Abs. 2 SigV: Dokumentation ist grundsätzlich mindestens weitere 30 Jahre ab dem Schluß des Jahres, in dem die Gültigkeit des Zertifikats endet aufzubewahren.	§ 8 Abs. 3 i.V.m. 4 Abs. 1 SigV: Dokumentation ist grundsätzlich 5 weitere Jahre ab Ende des Jahres, in dem die Gültigkeit des Zertifikats endet, aufzubewahren.
Einstellung des Betriebes oder Konkurs des Zertifizierungsdiensteanbieters	§ 13 Abs. 1 S. 2 SigG, § 15 Abs. 6 S. 1 SigG: Bemühen um Übernahme der gesamten Tätigkeit (einschließlich der gesperrten Zertifikate im Verzeichnis) durch anderen akkreditierten Anbieter durch Anbieter oder RegTP (§ 15 Abs. 6 S. 1 SigG). Gelingt dies nicht, muss der Zertifizierungsdiensteanbieter die gültigen Zertifikate nach § 13 Abs. 1 S. 2 SigG sperren und diese sowie die Dokumentation an die RegTP übergeben. § 15 Abs. 6 S. 3, § 10 Abs. 1 S. 1 SigG; § 8 Abs.3, § 4 Abs.2 SigV: Aufbewahrung der Dokumentation durch RegTP sowie Überprüfbarkeit der Daten bis zu 30 Jahre nach Gültigkeitsende gewährleistet.	§ 13 Abs. 1 S. 2 SigG: Anbieter muss dafür Sorge tragen, dass Dokumentation und gültige Zertifikate von einem anderen Anbieter übernommen werden. Keine Bemühungen der RegTP geboten. Neuer Anbieter muss nur gültige Zertifikate übernehmen (nicht die gesperrten). Kann kein anderer Anbieter gefunden werden, muss der Zertifizierungsdiensteanbieter die gültigen Zertifikate sperren (§ 13 Abs.1 S. 2 SigG) und die Dokumentation an die RegTP übergeben. § 8 Abs. 3 S. 1, § 4 Abs. 3 SigV: Aufbewahrung der Dokumentation durch RegTP bis 5 Jahre nach Fälligkeitsende gewährleistet sowie § 13 Abs. 2 S. 3 SigG: Auskunftserteilung über Zertifikate nur bei Vorliegen eines berechtigten Interesses und soweit technisch ohne unverhältnismäßig großen Aufwand möglich.
Haftung der Zertifizierungsdiensteanbieter (ZDA)	Haftung zwischen ZDA und Signaturschlüsselinhaber nach allgemeinen Grundsätzen. § 11 Abs. 1 SigG: Haftung gegenüber Dritten. § 12 SigG, § 9 SigV: Deckungsvorsorge.	Haftung zwischen ZDA und Signaturschlüsselinhaber nach allgemeinen Grundsätzen. § 11 Abs. 1 SigG: Haftung gegenüber Dritten. § 12 SigG, § 9 SigV: Deckungsvorsorge.

	"akkreditierte Signatur"	"qualifizierte Signatur"
Anerkennung ausländischer Signaturen und Produkte	Signaturen: § 23 Abs. 2 SigG bei vorherigem Nachweis einer gleichwertigen Sicherheit, Feststellung durch RegTP (§ 18 Abs. 2 SigV). Produkte: § 15 Abs. 8 SigG bei Nachweis einer gleichwertigen Sicherheit, Feststellung durch RegTP (§ 18 Abs. 3 SigV).	Signaturen: § 23 Abs. 1 SigG: automatische Gleichstellung von Produkten. Produkte: § 23 Abs. 3 SigG: Anerkennung, wenn in einem EU-Mitgliedstaat oder Vertragsstaat über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie entsprechen.
Zertifizierungsstruktur	§ 16 Abs. 1 SigG: Wurzelzertifikate der RegTP, welche die Vertrauenswürdigkeit der Zertifikatskette sichert. Zertifikate aller akkreditierten Anbieter befinden sich in gleicher Zertifizierungsstruktur, d.h. leichtere Interoperabilität.	Freie Wahl der Zertifizierungsstruktur durch Zertifizierungsdiensteanbieter. Keine gemeinsame Struktur mit anderen Anbietern; gegenseitige Anerkennung für Prüfmöglichkeit erforderlich Drohende Unübersichtlichkeit und eingeschränkte Interoperabilität.

Sind die Vorgaben des SigG und der SigV im Verhältnis zur europäischen Signaturrichtlinie abschließend für die nationale Verwaltung?

Nach Verabschiedung der europäischen Signaturrichtlinie wurden das deutsche SigG und die SigV an die europäischen Anforderungen angepasst. Das 2001 novellierte und in Kraft getretene SigG sowie die ebenfalls novellierte SigV entsprechen nun den gemeinschaftsrechtlichen Vorgaben zur Harmonisierung der einzelnen nationalen Gesetze. Nach ganz h.M. ist damit die Umsetzung der Signaturrichtlinie in das deutsche Recht vollständig erfolgt, so dass sich auch keine weiteren zu beachtenden Vorgaben aus der europäischen Richtlinie ergeben.

Weiterführende Literatur:
Einführend zur elektronischen Signatur: *Roßnagel,* Das neue Recht elektronischer Signaturen, NJW 2001, 1817*; Roßnagel*, Die neue Signaturverordnung, BB 2002, 261*; Roßnagel*, Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 215. Zur Nutzung der elektronischen Signatur in der Verwaltung*: Deutscher Städtetag* (Hrsg.), Welche elektronische Signatur braucht die Kommunalverwaltung?, Köln, Dezember 2001*; KoopA/ADV* (Hrsg.), Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung, Stand September 2002, abrufbar unter http://www.koopa.de/Arbeitsgruppen/kommunikation/koopAgesamt.pdf. Zur Funktionsäquivalenz zwischen handschriftlicher und elektronischer Signatur*: Schreiber*, Elektronisches Verwalten. Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, 2002, S. 76ff.*; Eifert,* Online-Verwaltung und Schriftform im Verwaltungsrecht, K&R, Beilage 2 zu Heft 10/2000, S. 11 (13ff.); *Roßnagel* (Hrsg.), Die elektronische Signatur in der Verwaltung, 2002. Zur Funktionsweise der elektronischen Signatur siehe *RegTP,* Referat IS 15 (Hrsg.), Die digitale Signatur, abrufbar unter www.regtp.de

6.3.4 Welche Regelungsaspekte gelten für Rahmenverträge zwischen Verwaltung und privaten Zertifizierungsdiensteanbietern?

In der Regel wird die Verwaltung nicht selbst als Anbieterin von Zertifizierungsdienstleistungen auftreten (vgl. hierzu oben S. 20). Daher wird sie zumindest teilweise oder häufig auch vollständig die Leistungen privater Zertifizierungs-

dienstleister in Anspruch nehmen, um die Mitarbeiter mit elektronischen Signaturen auszustatten. Hierfür bietet es sich an, die wesentlichen Bedingungen für eine Zertifizierung der Behördenmitarbeiter in einem Rahmenvertrag festzuhalten. Wie die Anforderungen der Verwaltung für die Zertifizierungsdienste ausgestaltet werden, hängt wesentlich von der konkreten organisatorischen Aufgabenverteilung zwischen Verwaltung und Privaten ab, ob also z.B. der gesamte Bereich der Zertifizierung durch Private erbracht werden soll oder Teile hiervon (z.B. die Registrierung) bei der Verwaltung verbleiben. Folgende Regelungsaspekte sollten aber mindestens umfasst werden:

- Regelungen zur Kostenübernahme für alle Zertifikate der Behördenmitarbeiter;
- Festlegung der Inhalte der Zertifikate (vgl. hierzu unten S. 72);
- Bei einem Zusammenwirken von Verwaltung und privaten Anbietern: Regelungen zur Verteilung der Haftungsrisiken zwischen den Parteien und ggf. Vorgaben für das Sicherheitskonzept.

6.3.5 Welche Vorgaben bestehen für den Inhalt von Zertifikaten?

Entsprechend der Legaldefinition in § 2 Nr. 6 SigG sind Zertifikate "elektronische Bescheinigungen, mit denen Signaturschlüssel einer Person zugeordnet werden und die Identität der Person bestätigt wird." An dieser Funktion des Zertifikats orientieren sich sowohl die Pflicht- als auch die freiwilligen Angaben in einem qualifizierten Zertifikat.

Was müssen qualifizierte Zertifikate zwingend enthalten?

Der gesetzlich vorgeschriebene Inhalt eines qualifizierten Zertifikats einer elektronischen Signatur ergibt sich aus § 7 Abs. 1 SigG. Hiernach muss ein qualifiziertes Zertifikat (**Hauptzertifikat**) folgende Angaben enthalten:

- gem. § 7 Abs. 1 Nr. 1 SigG den **Namen des Signaturschlüssel-Inhabers** (Vorname und Familienname) bzw. ein dem Signaturschlüssel-Inhaber zugeordnetes **unverwechselbares Pseudonym** i.S.v. § 5 Abs. 3 SigG. Im Falle einer Verwechslungsgefahr (z.B. bei Namensgleichheit) ist zudem ein **Namenszusatz** beizufügen (z.B. Adresse, Geburtsdatum oder Ordnungsziffer), der die Eindeutigkeit des Zertifikats sicherstellt;
- gem. § 7 Abs. 1 Nr. 2 SigG **den zugeordneten Signaturprüfschlüssel** sowie gem. § 7 Abs. 1 Nr. 3 SigG die **Bezeichnung der Algorithmen**, mit denen der Signaturprüfschlüsssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann;
- gem. § 7 Abs. 1 Nr. 4 SigG die **laufende Nummer des Zertifikats** zur eindeutigen Identifikation des Zertifikats im Verzeichnisdienst des Zertifizierungsdiensteanbieters und gem. § 7 Abs. 1 Nr. 5 SigG **Beginn und Ende der Gültigkeit des Zertifikats** (Datum und Uhrzeit);
- gem. § 7 Abs. 1 Nr. 6 SigG den **Namen des Zertifizierungsdiensteanbieters** und den **Namen des Staates**, in dem er niedergelassen ist;
- gem. § 7 Abs. 1 Nr. 7 SigG Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte **Anwendungen nach Art oder Umfang beschränkt** ist, z.B. Begrenzung auf bestimmte dienstliche Aufgaben oder finanzielle Höchstgrenzen für elektronische Transaktionen;
- und letztlich aus Gründen der Transparenz Angaben darüber, dass es sich um ein **qualifiziertes Zertifikat** handelt.
- Werden Zertifikate für die Signatur elektronischer Verwaltungsakte eingesetzt, sind die sich aus **§ 37 Abs. 3 S. 2 VwVfG** zusätzlich ergebene Inhaltspflichten zu beachten, denn hiernach muss auch ein elektronischer Verwaltungsakt z.B. die erlassene Behörde erkennen lassen. Siehe für die hierfür notwendigen Pflichtangaben S. 76.

Gem. § 14 Abs. 1 SigV müssen die Angaben nach § 7 Abs. 1 SigG **eindeutig** sein. Der gesetzlich vorgeschriebene Inhalt zwischen qualifizierten und akkreditierten Signaturen unterscheidet sich hierbei nicht. Denn auch akkreditierte Signaturen sind qualifizierte Signaturen, allerdings mit dem Zusatz, dass sich hier der Diensteanbieter einer freiwilligen Akkreditierung nach § 15 SigG unterworfen hat.

Was können Signatur-Zertifikate zusätzlich enthalten?

Zusätzlich zu den Pflichtangaben im Zertifikat nach § 7 Abs. 1 Nr. 1-8 SigG kann ein qualifiziertes Zertifikat nach Bedarf zusätzliche Angaben (sog. **Attribute**) des Signaturschlüssel-Inhabers beinhalten. Gem. § 5 Abs. 2 SigG sind dies z.B.

Angaben über die Vertretungsmacht des Signaturschlüssel-Inhabers, **berufsbezogene** oder **sonstige Angaben zur Person**. Für Bedienstete der Verwaltung besteht z.B. die Möglichkeit, Zugehörigkeit zu einer spezifischen Behörde, Dienststelle oder Abteilung aufzunehmen, sowie Auskunft über Zeichnungsberechtigungen und weitere Kompetenzen zu geben.
Diese weiterführenden Angaben können gem. § 7 Abs. 2 SigG auch in ein gesondertes qualifiziertes Zertifikat (sog. **qualifiziertes Attribut-Zertifikat**) aufgenommen werden. Dies hat den Vorteil, dass der Signierende nur bei individuellem Bedarf eine Signatur mit erweiterten Angaben zu erstellen braucht, ansonsten aber im Regelfall alleine auf das Hauptzertifikat mit den Pflichtangaben zurückgreifen kann. Für die Nutzung von Signaturschlüsseln innerhalb der Verwaltung entstehen hierdurch erweiterte Möglichkeiten für ein sinnvolles Key-Management. Vgl. zum Einsatz von Attributzertifikat im Key-Management unten S. 88.
Wird ein qualifiziertes Attribut-Zertifikat ausgestellt, muss dieses jedoch erneut bestimmte Pflichtangaben enthalten, die sich aus § 14 Abs. 2 SigV ergeben. Hiernach muss ein qualifiziertes Attribut-Zertifikat i.S.v. § 7 Abs. 2 SigG neben einer **eindeutigen Referenz auf das zugrunde liegende qualifizierte Zertifikat** folgende Angaben enthalten:

- gem. § 14 Abs. 2 Nr. 1 SigV die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüsssel des Zertifizierungsdiensteanbieters benutzt werden kann sowie gem. § 14 Abs. 2 Nr. 2 SigV die Nummer des Attribut-Zertifikats;
- gem. § 14 Abs. 2 Nr. 3 SigV den Namen des Zertifizierungsdiensteanbieters und den Namen des Staates , in dem er niedergelassen ist sowie gem. § 14 Abs. 2 Nr. 4 SigV Angaben darüber, dass es sich um ein qualifiziertes Zertifikat handelt.

Was ist durch die Verwaltung bei einer Beantragung von Zertifikaten zu beachten?

Möchte die Verwaltung weiterführende Angaben im Hauptzertifikat oder in einem Attributzertifikat aufnehmen lassen, bestehen hierfür abhängig von der Art der konkreten Angabe bestimmte Anforderungen. So ist für Angaben über die Vertretungsmacht für eine dritte Person gem. § 5 Abs. 2 S. 2 SigG die **Einwilligung** dieser Person nachzuweisen. Sollen Zertifikate berufsbezogene oder sonstige Angaben enthalten, so sind diese gem. § 5 Abs. 2 S. 2 SigG durch die jeweils hierfür **zuständige Stelle zu bestätigen** (z.B. durch den Arbeitgeber oder die Dienststelle). Liegt im Falle der Vertretungsmacht keine gültige Einwilligung und hinsichtlich weiterer Angaben keine gültige Bestätigung vor, so dürfen diese Angaben nicht in ein qualifiziertes Zertifikat aufgenommen werden. Alle weiterführenden **personenbezogenen Angaben** dürfen schließlich in ein qualifiziertes Zertifikat **nur mit Einwilligung des Betroffenen** aufgenommen werden.

Was ist durch die Verwaltung bei einer nachträglichen Unrichtigkeit von Zertifikaten zu beachten?

Wechselt ein Bediensteter der Verwaltung die Dienststelle oder Abteilung, werden entsprechende Angaben über die Vertretungsbefugnis oder berufsbezogene Angaben im Haupt- oder Attributzertifikat ggf. unrichtig. Um Signaturen mit unrichtigen Zertifikaten zu vermeiden, ist in einem solchen Fall die **Sperrung** des qualifizierten Zertifikats oder des Attributzertifikats beim Zertifizierungsdiensteanbieter zu beantragen. Der Zertifizierungsdiensteanbieter hat gem. § 8 Abs. 1 S. 1 SigG ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt oder das Zertifikat bereits aufgrund falscher Angaben zu § 7 SigG ausgestellt wurde. Beinhaltet ein qualifiziertes Zertifikat bzw. ein Attributzertifikat Angaben i.S.v. § 5 Abs. 2 SigG (vgl. hierzu oben S. 73) kann gem. § 8 Abs. 2 SigG auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle bei nachträglicher Unrichtigkeit eine Sperrung gem. § 8 Abs.1 SigG beantragen. Ergeben sich Änderungen für die Angaben von Bediensteten, sollte daher i.d.R. auch der Dienstherr selbst bzw. die für die Koordination des Key-Management zuständige Stelle, eine Sperrung des unrichtigen Zertifikats beantragen.

6.3.6 Ist auch die Verwendung von Software-Signaturen zulässig?

Für die Sicherheitsstruktur eines qualifizierten Signaturverfahrens ist es wesentlich, dass der private Schlüssel **geheim gehalten** wird und nur mittels einer ebenfalls geheimen Personenidentifikation für die Erstellung einer Signatur genutzt werden kann. Denn gem. § 2 Nr. 2 a SigG ist die elektronische Signatur mit Mitteln zu erzeugen, die der Signaturschlüssel-Inhaber unter seiner **alleinigen Kontrolle** halten kann. Bereits hieraus ergeben sich erhöhte Sicherheitsanforderungen an Signaturerstellungseinheiten.

Nur für Signaturerstellungseinheiten einer qualifizierten elektronischen Signatur konkretisiert das SigG in Verbindung mit der SigV jedoch die Anforderungen, welche erfüllt sein müssen, um den Kriterien aus § 2 Nr. 2 SigG gerecht zu werden. Die Anforderungen an Produkte für qualifizierte elektronische Signaturen sind in § 17 SigG geregelt. Die erforderlichen **Spezifikationen für sichere Erstellungseinheiten** i.S.v. § 17 Abs. 1 SigG enthält § 15 SigV. In der amtlichen Begründung zu § 15 SigV wird festgestellt, dass eine sichere Signaturerstellungseinheit in der Regel in Form einer Chipkarte erfolgen wird. Denn § 15 Abs. 1 S. 2 SigV erfordere für sichere Signaturerstellungseinheiten, dass der Signaturschlüssel nicht aus der sicheren Signaturerstellungseinheit exportiert werden könne. Um mögliche Vervielfältigungen des Signaturschlüssels zu verhindern, wird eine Anwendungssicherung durch **alleinigen Besitz an der Chipkarte** realisiert. Software-Signaturen für Einzel-PCs des Bürgers entsprechen daher i.d.R. gerade nicht diesen erhöhten Sicherheitsanforderungen. Bei Sicherheitsboxen wird der Schutzfunktion durch individuellen Besitz dadurch entsprochen, dass nur berechtigte Personen Zugang zur Signaturkomponente erhalten.

Software-Signaturen bieten daher auf Seiten des Bürgers zur Zeit kein taugliches Signaturverfahren, um den Anforderungen einer qualifizierten elektronischen Signatur zu entsprechen und gesetzlichen Formerfordernisses gerecht zu werden. Auf Seiten der Verwaltung erfüllen Software-Signaturen nur in Verbindung mit sog. **Sicherheitsboxen** die Anforderungen einer qualifizierten elektronischen Signatur (vgl. S. 89). Es handelt sich hierbei um Kryptoprozessoren, welche sämtliche Sicherheitsfunktionen einer Chipkarte erfüllen und in Massensignaturverfahren auch innerhalb der Verwaltung Anwendung finden können.

Weiterführende Literatur:
Vgl. zur Rolle der Behörden im Zertifizierungsverfahren *Roßnagel* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002, S. 53ff.. Zur Verwendung von Hauptzertifikaten: *Schreiber*, Elektronisches Verwalten: Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, 2002, S. 128ff. Zur Verwendung von Attributzertifikaten: *ders.*, S. 140ff. Zu dem Erfordernis einer Chipkarte als sichere Signaturerstellungseinheit: *Roßnagel/Pordsch* in Roßnagel (Hrsg.), Recht der Multimedia-Dienste, Loseblatt-Kommentar, Stand Nov. 2000, SigV, § 16 Rnr. 58ff. Zur Verwendung einer Sicherheitsbox als Signaturserver: *Schreiber*, Elektronisches Verwalten: Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, 2002, S. 150ff.

6.3.7. Welche Beweiskraft haben Dokumente mit elektronischer Signatur?

Die Beweiskraft aller elektronischen Signaturen im gerichtlichen Verfahren unterliegt grundsätzlich der freien richterlichen Beweiswürdigung. § 371 Abs. 1 S. 2 ZPO sieht hierfür vor, dass elektronische Dokumente im Prozess als Augenscheinbeweis anzusehen sind. § 292a ZPO bestimmt als Form der Beweiserleichterung für elektronische Dokumente mit qualifizierter elektronischer Signatur das Bestehen eines Anscheinsbeweises. Gegenüber sonstigen elektronischen Dokumenten sind solche mit qualifizierter elektronischer Signatur also privilegiert. Gem. § 292a ZPO soll der Erklärungsempfänger den Beweis, dass Signaturschlüsselinhaber und Erklärender identisch sind, bereits bei Konformität der Signatur mit den Anforderungen des SigG erbringen können. Dieser Anschein der Echtheit kann nur durch die Darlegung von Tatsachen erschüttert werden, die ernstliche Zweifeln daran begründen, dass die Erklärung mit dem Willen des Signaturschlüsselinhabers abgeben worden ist. Auch wenn kein Schriftformerfordernis vorliegt, kommt einem elektronischen Dokument mit qualifizierter elektronischer Signatur von einem akkreditierten oder nicht akkreditierten Diensteanbieter daher eine erhöhte Beweiskraft zu. Allerdings ist zu beachten, dass die Anbieter von qualifizierten Signaturen zunächst nur glaubhaft machen müssen, die Anforderungen des SigG einzuhalten und damit auch tatsächlich qualifizierte elektronische Signaturen anzubieten. Überprüft ist dies nur bei qualifizierten elektronischen Signaturen eines akkreditierten Diensteanbieters. Nicht signierten elektronischen Dokumenten misst die Rspr. dagegen meist kaum Beweiskraft zu.

Auch im Verwaltungsverfahren sind elektronische Dokumente geeignete Beweismittel i.S.d. § 26 VwVfG für die Sachverhaltsermittlung. Mit dem Einfügen der Wörter "*oder elektronisch*" in § 26 Abs. 1 S. 2 Nr. 2 VwVfG stellte der Gesetzgeber mit dem 3. VwVf-ÄndG zudem klar, dass die Verwaltung auch auf elektronischem Wege Äußerungen von Beteiligten, Sachverständigen und Zeugen einholen kann. Das Verwenden einer qualifizierten elektronischen Signatur ist hierfür nicht erforderlich. Allerdings dürfte sich in Zweifelsfällen die Beweiskraft eines elektronischen Dokuments im Vergleich mit "klassischen Beweismitteln" durch die Verwendung einer qualifizierten elektronischen Signatur erhöhen.

Weiterführende Literatur:
Zur Beweiseignung elektronischer Signaturen: *Roßnagel*, Rechtliche Unterschiede von Signaturverfahren, MMR 2002, S. 215 (217f.). Zum Beweiswert elektronischer Dokumente: *Vehslage*, Beweiswert elektronischer Dokumente, K&R 2002, S. 531ff.; *Fischer-Dieskau/Gitter/Paul/Steidle*, Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, S. 709ff. Zur fehlenden Beweiseignung von E-Mail siehe *Roßnagel/Pfitzmann*, Der Beweiswert von E-Mail, NJW 2003, i.E.

6.3.8. Bestehen beim unbefugten Einsatz der Signaturkarte mit PIN durch einen Dritten Haftungsrisiken für die Verwaltungsbediensteten?

Werden die Verwaltungsbediensteten mit individuellen elektronischen Signaturen ausgestattet, erhalten sie eine mit dem privaten Schlüssel versehene Signaturkarte, die gegenwärtig nur in Verbindung mit einer geheimen PIN eingesetzt werden kann. Wird die Signaturkarte unter Verwendung der PIN missbräuchlich durch einen Dritten genutzt und entsteht daraus ein Schaden, stellt sich die Frage, inwiefern der Verwaltungsbedienstete für den Schaden haftet.

Im **Außenverhältnis** bestimmt sich die Haftung nach den allgemeinen Regeln der Amtshaftung bzw. der deliktsrechtlichen Haftung. Regelmäßig **haftet** danach die **Körperschaft**, außer sie kann sich in begrenzten Ausnahmefällen exkulpieren.

Ein haftungsrechtlicher **Rückgriff** der Körperschaft gegenüber **dem Verwaltungsbediensteten** kommt nach Beamtenrecht (vgl. z.B. § 46 Beamtenrechtsrahmengesetz, § 78 Bundesbeamtengesetz, Art. 85 Bayrisches Beamtengesetz) bzw. den Tarifverträgen für Arbeitnehmer im öffentlichen Dienst (vgl. z.B. § 14 Bundesangestellten-Tarifvertrag) nur in Betracht, wenn der Verwaltungsbedienstete **vorsätzlich oder grob fahrlässig** einem Dritten die Verwendung seiner Signaturkarte mit PIN ermöglicht hat. Für den anzulegenden Sorgfaltsmaßstab kommt es dabei immer auf eine Betrachtung des Einzelfalles an. Als Orientierung für die generellen Sorgfaltsanforderungen können die von den Gerichten entwickelten Grundsätze für den Missbrauch von EC-Karten bzw. Kreditkarten mit PIN herangezogen werden und sind die Dienstanweisungen zu beachten. Im Ergebnis kommt ein grob fahrlässiges Verhalten des Verwaltungsbediensteten jedenfalls in der Regel immer dann in Betracht, wenn die **PIN und Signaturkarte gemeinsam aufbewahrt** werden.

Weiterführende Literatur:
Allgemein: *Ebert*, Das gesamte öffentliche Dienstrecht für Beamte, Angestellte und Arbeiter bei Bund, Ländern und Kommunen, 2. Aufl. 1995, Lieferung Stand Nov. 2002, Kennzahl 270 S. 16ff. Zum Missbrauch bei EC-Karten/ Kreditkarten mit PIN: *Janisch/Schartner*, Internetbanking - Sicherheitsaspekte und Haftungsfragen, DuD 2002, S. 162ff.

6.3.9. Müssen Anlagen zu einem signierten Antrag ebenfalls signiert werden?

Ob Anlagen zu einem Antrag, für den das Schriftformerfordernis gilt, ebenfalls mit einer qualifizierten elektronischen Signatur versehen werden müssen, bestimmt sich nach der Reichweite des konkreten Schriftformerfordernisses. Bezieht dieses nach Sinn und Zweck der Vorschrift die Anlagen zum Antragsdokument mit ein, so müssen auch diese entsprechend § 3a Abs. 2 VwVfG mit einer qualifizierten elektronischen Signatur unterzeichnet werden, um dem gesetzlichen Schriftformerfordernis zu entsprechen. Dies ist z.B. dann der Fall, wenn sich der Inhalt des Antrags erst im vollen Umfang aus den beigefügten Anlagen erschließen lässt, so dass diese faktisch Teil des Antrages werden. Auch ansonsten ist der Einsatz der qualifizierten elektronischen Signatur zum Schutz der Integrität der Anlagen und der Beweissicherung zu empfehlen.

6.3.10. Wie können elektronische Dokumente durch die Behörde beglaubigt werden?

§ 33 VwVfG regelt die Anforderungen an amtliche Beglaubigungen. Ebenso wie öffentliche Beurkundungen und Beglaubigungen dienen sie der Sicherheit im Rechtsverkehr. Sie geben Auskunft über die Echtheit einer Abschrift oder Unterschrift, nicht jedoch über die Richtigkeit des Inhalts der Erklärung. Durch das 3. VwVf-ÄndG wurden die Regelungen des § 33 VwVfG auch an den modernen Rechtsverkehr angepasst. Erfasst werden drei unterschiedliche Fallkonstellationen, in denen elektronische Dokumente beglaubigt werden können:

- Bei der **Beglaubigung des Ausdrucks eines elektronischen Dokuments**, das mit einer qualifizierten elektronischen Signatur versehen ist, müssen neben den allgemeinen Anforderungen an eine Beglaubigung gem. § 33 Abs. 5 Nr. 1 a-c VwVfG zusätzlich Angaben darüber ausgestellt werden, wen die Signaturprüfung als Inhaber der Signatur ausweist; welchen

Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist und welche Zertifikate mit welchen Daten der Signatur zugrunde lagen.

- Bei der **Beglaubigung eines in elektronische Form überführten Papierdokuments** muss der Beglaubigungsvermerk gem. § 33 Abs. 5 Nr. 2 S. 1 VwVfG zusätzlich zu den allgemeinen Angaben auch den Namen des für die Beglaubigung zuständigen Bediensteten sowie die Bezeichnung der Behörde, die die Beglaubigung vornimmt, enthalten. Die erforderliche Unterschrift und das Dienstsiegel sind durch eine dauerhaft überprüfbare qualifizierte elektronische Signatur i.S.v. § 37 Abs. 4 VwVfG zu ersetzen (zur Zeit erfordert dies die Signatur mit qualifizierten Zertifikat eines akkreditierten Zertifizierungsdienstes i.S.v. § 15 SigG).
- Wird ein bereits in elektronischer Form vorhandenes, jedoch **umformatiertes Dokument** beglaubigt, so müssen auch hier die Anforderungen an einen Begläubigervermerk i.S.v. § 33 Abs. 5 Nr. 2 S. 1 VwVfG vorliegen. Zusätzlich tritt auch hier das Erfordernis hinzu, die Ergebnisse der Signaturprüfung entsprechend der Regelung in Satz 1 Nr. 1 beizufügen.

Stellt sich bei der Prüfung der elektronischen Signatur heraus, dass sie fehlerhaft ist, so kann dies unmittelbar zu einem **Beglaubigungsverbot** führen. Denn gem. § 33 Abs. 2 VwVfG dürfen Abschriften nicht beglaubigt werden, wenn Umstände zu der Annahme berechtigen, dass der ursprüngliche Inhalt des Schriftstückes, dessen Abschrift beglaubigt werden soll, geändert worden ist. Dies wird insbesondere dann der Fall sein, wenn die Integrität des zu beglaubigende Dokuments durch die elektronische Signatur nicht mehr sicher nachweisbar ist.

Weiterführende Literatur:
Begründung des Entwurfes eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften, BT-Drs. 14/9000, S. 32f. Zur amtlichen Beglaubigung allgemein *Bonk/Kallerhoff* in: Stelkens/Bonk/Sachs, Kommentar zum VwVfG, § 33.

6.4. Was ist durch die Verwaltung bei elektronischen Verwaltungsakten zu beachten?

6.4.1. Sind elektronische Verwaltungsakte nur mit elektronischer Signatur zulässig?

Grundsätzlich gilt auch für elektronische Verwaltungsakte der **Grundsatz der Formfreiheit**. Die Behörde kann daher gem. § 37 Abs. 2 VwVfG im Rahmen einer rechtmäßigen Ausübung ihres Ermessens einen Verwaltungsakt mündlich, schriftlich, elektronisch oder in anderer Weise erlassen. Besondere Anforderungen sind hieran nicht geknüpft. Ähnlich wie bei schriftlichen Verwaltungsakten muss auch der elektronische Verwaltungsakt gem. § 37 Abs. 3 VwVfG lediglich die erlassende Behörde erkennen lassen und die Unterschrift oder die Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten. Auch ohne qualifizierte elektronische Signatur sind solche Verwaltungsakte zulässig. Etwas anderes gilt dann, wenn für den Erlass eines Verwaltungsaktes ein gesetzliches Schriftformerfordernis besteht. Dann ist im Regelfall entsprechend § 3a Abs. 2 VwVfG eine qualifizierte elektronische Signatur zwingend erforderlich. Gem. § 37 Abs. 3 S. 2 VwVfG muss hierbei das der Signatur zugrunde liegende qualifizierte Zertifikat oder ein zugehöriges qualifiziertes Attributzertifikat auch die erlassende Behörde erkennen lassen (vgl. zum notwendigen Inhalt von oben Zertifikaten S. 72). Zudem ermöglicht § 37 Abs. 4 VwVfG, dass für die qualifizierte elektronische Signatur eines elektronischen Verwaltungsaktes durch Rechtsverordnung die dauerhafte Überprüfbarkeit angeordnet wird (hierzu vgl. S. 80).

6.4.2. Ist eine gesonderte elektronische **Rechtsbehelfsbelehrung** formgebunden?

Für schriftlich erlassene Verwaltungsakte besteht die **Pflicht zur Rechtsbehelfsbelehrung**. Diese hat in **schriftlicher Form** zu erfolgen. Wird ein elektronischer Verwaltungsakt erlassen, mit dem auch einem gesetzlichen Schriftformerfordernis genüge getan werden soll, so ist dieser daher ebenfalls mit einer Rechtsbehelfsbelehrung zu versehen. Beide sind mit einer qualifizierten elektronischen Signatur zu signieren. Eine gesetzliche Pflicht, einen "einfachen" elektronischen Verwaltungsakt mit einer Rechtsmittelbelehrung zu versehen, besteht dagegen nicht. Wird ein Verwaltungsakt ohne Rechtsbehelfbelehrung zugestellt und bekannt gegeben, ist jedoch die verlängerte Widerspruchsfrist von einem Jahr gem. § 58 Abs. 2 VwGO zu beachten. Daher kann es auch im Interesse der Verwaltung liegen, einen formlosen elektronischen Verwaltungsakt mit einer elektronischen Rechtsbehelfsbelehrung zu versehen. Es ist noch nicht abschließend geklärt, ob diese dann eine qualifizierte elektronische Signatur erfordert. Teilweise wird dies aus § 3a VwVfG abgeleitet, der aufgrund des direkten Bezuges zum Verwaltungsverfahren und seiner Stellung im

Gesetz auch hier Anwendung finden soll. Mit der Funktion der Schriftform als Ausgangspunkt einer funktionsgerechten Auslegung wären jedoch auch geringere Anforderungen an die elektronische Form einer Rechtsbehelfsbelehrung denkbar. Der hier im Vordergrund stehenden Dokumentationsfunktion schriftlicher Dokumente dürfte bereits mit einem einfachen Attachment zur E-Mail entsprochen werden.
Angesichts der rechtlichen Unsicherheit wird empfohlen, die Gefahr einer Rechtsunwirksamkeit mit der Folge verlängerter Fristen durch die Verwendung von qualifizierten elektronischen Signaturen zu vermeiden. Dies gilt auch für solche Fälle der elektronischen Rechtsbehelfsbelehrung, in denen ein Verwaltungsakt ohne Formerfordernis elektronisch erlassen wird.

6.4.3. Welche Anforderungen bestehen hinsichtlich des Zugangs von elektronischen Erklärungen oder Verwaltungsakten?

Der Zugang einer elektronischen Erklärung bzw. eines elektronischen Verwaltungsaktes kann zunächst gem. § 3a Abs. 1 VwVfG nur erfolgen, wenn der Bürger den Zugang für elektronische Dokumente grundsätzlich eröffnet hat (**Zugangseröffnung**). Gleiches gilt für den Zugang von elektronischen Anträgen etc. auf Behördenseite. Weitere Regelungen über den Zugang von elektronisch übermittelten Willenserklärungen soll auch § 3a Abs. 3 VwVfG jedoch nicht treffen. Hierfür wird in der Gesetzesbegründung zum 3. VwVf-ÄndG ausdrücklich auf die allgemeinen Regelungen des Verwaltungsverfahrensrechts verwiesen. Bei Anwendung dieser allgemeinen Grundsätze muss bei der Beurteilung des Zugangs elektronischer Erklärungen zwischen Zugang auf Seite der Behörde und Zugang auf Seite des Bürgers unterschieden werden.

Was gilt allgemein für den Zugang auf Seiten der Behörde?

Allgemein gilt eine Willenserklärung oder ein Antrag auf Seiten der Behörde in analoger Anwendung des Grundsatzes aus § 130 BGB als zugegangen, wenn er in die Verfügungsgewalt der Behörde gelangt ist und bei gewöhnlichem Verlauf und normaler Gestaltung der Verhältnisse mit der Kenntnisnahme durch die Verwaltung zu rechnen ist. Dieser Grundsatz gilt gleichfalls für den Zugang von elektronischen Willenserklärungen. Werden elektronische Kommunikationssysteme für die Abgabe von Erklärungen, Anträgen etc. verwendet, so genügt daher der Eingang des elektronischen Dokuments in den elektronischen Postkasten der zuständigen Behörde, ohne dass diese die elektronische Willenserklärung tatsächlich zur Kenntnis genommen haben muss. Entscheidend ist, wann mit einer Leerung des elektronischen Postkastens der Behörde gerechnet werden durfte (i.d.R. werktäglich). Ein Nachweis des Zugangs sollte über die Verwendung eines elektronischen Zeitstempels oder über eine elektronische Eingangsbestätigung erfolgen. Anderes ergibt sich dagegen für den Fall, dass ein Antragsteller mit Übermittlung des elektronischen Dokuments eine Frist zu wahren hat. Da dem Antragsteller im Verwaltungsverfahren das Recht zusteht, Fristen voll auszunutzen, kann hier nicht die Kenntnisnahme im Rahmen des üblichen Verlaufes als ausschlaggebend angesehen werden. Vielmehr ist ausschließlich das tatsächliche Gelangen z.B. eines elektronischen Antrags in die Verfügungsgewalt der Behörde beachtlich. Läuft eine Frist um 24 Uhr ab, kann diese also auch noch durch Eingang des elektronischen Dokuments in den elektronischen Postkasten um 23.59 Uhr gewahrt werden.
Als nicht zugegangen gelten elektronische Dokumente, die in **nicht lesbarer Form** übersendet werden. Hier besteht keine Möglichkeit der Behörde zur Kenntnisnahme. Zu beachten ist allerdings, dass für die Behörde mit § 3a Abs. 3 VwVfG die ausdrückliche gesetzliche Verpflichtung zur Information des Bürgers normiert wurde, sollte ein elektronisch übermitteltes Dokument nicht zur Bearbeitung geeignet sein. Teilweise wird hierzu vertreten, dass eine Verletzung dieser Pflicht eine Zugangsfiktion auslösen kann. Dies ginge aber über die Regelungsabsicht des Gesetzgebers hinaus. In der Praxis wird es sich daher anbieten, schon im Rahmen der notwendigen Kommunikationseröffnung auf den jeweiligen elektronischen Datenstandard hinzuweisen. Für den Fall, dass ein in lesbarer Form zugegangenes Dokument nicht geöffnet wird oder eine regelmäßige Überprüfung des elektronischen Postfachs nicht stattfindet, kann dagegen auf das Gelangen des Dokuments in den Machtbereich des Empfängers abgestellt werden (s.o.).

Was gilt allgemein für den Zugang auf Seiten des Bürgers?

Auf Seiten des Bürgers sind hinsichtlich der Möglichkeit der Kenntnisnahme nicht dieselben Maßstäbe wie bei einer Behörde anzuwenden. Im Rahmen der **Verkehrsanschau-**

ung ist zu beachten, dass für den Privatbürger noch nicht zwingend von einer täglichen Leerung seines elektronischen Posteingangs auszugehen ist. Anders dagegen bei berufstätigen bzw. professionellen Anwendern (Rechtsanwälte, Architekten). Ähnlich wie bei der Verwaltung steht hier die dienstliche Kommunikation im Vordergrund, und kann von einer werktäglichen Leerung ausgegangen werden. Da letztlich erneut die Verkehrsanschauung entscheidend ist, können mit einer noch stärkeren Verbreitung des Mediums Internet im privaten Raum auch die Anforderungen an den Bürger steigen.

Auch hier wird teilweise vertreten, dass eine Zugangsfiktion eintritt, wenn der Bürger seine in § 3a Abs. 3 VwVfG verankerte Obliegenheit verletzt. Dem kann auch hier entgegen gehalten werden, dass § 3a Abs. 3 VwVfG gerade keine Regelungen des Zugangs treffen sollte.
Die Rechtsfolgen aus § 3a Abs. 3 VwVfG für die allgemeinen Grundsätze der Zustellung sind daher noch nicht abschließend geklärt. Um Unsicherheiten hinsichtlich der Frage des Zugangs zu vermeiden, sollte sowohl auf Seiten des Bürgers als auch auf Seiten der Behörde dem Gebot zur Information der Gegenseite nachgekommen werden. Fragen der fehlerhaften Zustellung und möglicher Pflichten aus § 3a Abs. 3 VwVfG können so auf ein Minimum reduziert werden.

Wann ist der elektronische Verwaltungsakt zugegangen?

Den Zugang eines elektronischen Verwaltungsaktes regelt **§ 41 Abs. 2 VwVfG** in seiner Neufassung. Hiernach gilt ein Verwaltungsakt, der elektronisch übermittelt wird, am dritten Tag nach der Absendung als bekannt gegeben (**Drei-Tages-Fiktion**). Dies soll dann nicht gelten, wenn der Verwaltungsakt nicht oder zu einem späteren Zeitpunkt zugegangen ist. In Zweifelsfällen trifft die Verwaltung die Beweislast. Die Regelung entspricht den Zugangsregeln für papierförmige Verwaltungsakte.

6.4.4. Wie kann eine Beweissicherung des Zugangs erfolgen?

Ebenso wie bei Ablauf eines "klassischen" Verwaltungsverfahrens in Papierform ist eine Zugangsbestätigung des Eingangs eines elektronischen Dokuments bei der Verwaltung meist nicht gesetzlich vorgeschrieben. Grds. trifft den Bürger die Beweislast über den fristgerechten Zugang seines Dokuments, unabhängig von der Form der Übermittlung. Wird eine Zugangsbestätigung aus Gründen der Bürgerfreundlichkeit erwünscht, kann die rechtsverbindliche Bestätigung des zeitlichen Zugangs eines elektronischen Dokuments durch **automatische elektronische Eingangsbestätigung via E-Mail** erfolgen, die ausgelöst wird, sobald das elektronische Dokument das Postfach der Behörde erreicht hat. Zur Beweissicherung kann behördenintern zusätzlich das automatische und gesicherte Versehen des elektronischen Dokuments mit einem elektronischen Eingangs- bzw. Zeitstempel erfolgen.
Gem. § 2 Nr. 14 SigG ist ein **qualifizierter elektronischer Zeitstempel** die elektronische Bescheinigung eines Zertifizierungsdiensteanbieters, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Der Zertifizierungsdiensteanbieter muss hierbei mindestens den Anforderungen der §§ 4 bis 14 sowie § 17 und § 23 des SigG und zugehörigen Vorschriften der SigV entsprechen. Wird ein Zeitstempel zur Beweissicherung benötigt, wird zumeist der Hash-Wert eines elektronischen Dokuments an einen Trustcenter geschickt, wo dieser mit einer verbindlichen rechtsgültigen Zeitangabe versehen und dem Absender wieder zurückgeschickt wird.

6.4.5. Welche Anforderungen bestehen an die elektronische Begründung eines Verwaltungsaktes?

Gem. § 39 Abs. 1 S. 1 VwVfG ist ein schriftlicher oder elektronischer sowie ein schriftlich oder elektronisch bestätigter Verwaltungsakt mit einer Begründung zu versehen. Die Begründung hat in der Form zu erfolgen, die für den vorangehenden Verwaltungsakt gilt ("*zu versehen*"). Ein elektronischer Verwaltungsakt ist daher auch elektronisch zu begründen. Eine qualifizierte elektronische Signatur ist für die elektronische Begründung nur erforderlich, wenn der elektronische Verwaltungsakt der Schriftform unterliegt; mit dem 3. VwVf-ÄndG wurde das ausdrückliche Erfordernis der Schriftform aus § 39 Abs. 1 S. 1 VwVfG gestrichen. Letztlich hat die elektronische Begründung nicht erneut den inhaltlichen Anforderungen des § 37 Abs. 3 S. 2 VwVfG Rechnung zu tragen, da diese Regelung nur für den Verwaltungsakt selbst gilt. Etwas anderes gilt allerdings dann, wenn die elektronische Begründung unterblieben ist und auf elektronischem Weg nachgeholt werden soll. Dann muss für den Empfänger zumindest die Möglichkeit beste-

hen, die Begründung dem vorhergegangenen Verwaltungsakt zuzuordnen und die handelnde Behörde zu erkennen.

6.4.6. Dürfen Verwaltungsakte auch elektronisch bestätigt werden?

Für die Frage der elektronischen Bestätigung eines Verwaltungsaktes ist zwischen mündlich erlassenen Verwaltungsakten, elektronisch erlassenen Verwaltungsakten ohne Schriftformerfordernis und elektronisch erlassenen Verwaltungsakten mit Schriftformerfordernis zu unterscheiden:

- **Mündlich erlassene Verwaltungsakte** sind durch die zuständige Behörde gem. § 37 Abs. 2 S. 2 VwVfG entweder **schriftlich oder elektronisch** zu bestätigen, wenn hieran ein berechtigtes Interesse besteht und der Betroffene dies unverzüglich verlangt. Eine qualifizierte elektronische Signatur ist für die elektronische Bestätigung eines mündlich erlassenen Verwaltungsaktes nicht erforderlich.
- Für die Bestätigung eines gem. § 37 Abs. 2 S. 1 VwVfG bereits formlos elektronisch erlassenen Verwaltungsakt besteht die Möglichkeit einer elektronischen Bestätigung selbst unter Verwendung einer qualifizierten elektronischen Signatur dagegen nicht. **Ein formloser elektronischer Verwaltungsakt ist folglich schriftlich zu bestätigen**, die Generalklausel des § 3a Abs. 2 VwVfG findet explizit keine Anwendung.
- Wurde ein Verwaltungsakt, für den ein gesetzliches Schriftformerfordernis besteht, aufgrund der Generalklausel des § 3a Abs. 2 VwVfG elektronisch und mit qualifizierter elektronischer Signatur erlassen, so besteht schon **keine Pflicht der Behörde zur Bestätigung**, da die elektronische Form hier ein vollständiges Äquivalent zur Schriftform darstellt.

6.4.7. Welche Anforderungen bestehen an eine elektronische Aktenführung?

Die **Erforderlichkeit ordnungsgemäßer Aktenführung** gilt auch bei digitalen Dokumenten und ergibt sich aus den allgemeinen Grundsätzen der Aktenführung, wie sie für die Akte in Papierform aus § 29 VwVfG entwickelt wurden. Für eine elektronische Vorgangsbearbeitung bedeutet dies, dass elektronische Verwaltungsunterlagen elektronisch registriert, digital abgespeichert und ebenso elektronisch abrufbar organisiert werden müssen. Die rechtlichen Kriterien der **Wahrheit und Vollständigkeit der Aktenführung** müssen auch bei digitaler Aktenführung eingehalten werden. Dies erfordert konkret, dass eine **zweifelsfreie Identifizierung** der elektronischen Dokumente möglich ist, elektronische Dokumente, die dasselbe Verfahren betreffen, auch als solche **Einheit** zu erkennen sind und ein System besteht, welches es zulässt, die Dokumente nach **formalen Kriterien** wieder zu finden. Auch ist kenntlich zu machen, wer in welcher Form auf die Entscheidung der Verwaltung Einfluss genommen hat. Schließlich ist sicherzustellen, dass nachträgliche Korrekturen an elektronischen Dokumenten für Dritte erkennbar sind und keine unbefugten Löschungen vorgenommen werden. Die genannten Anforderungen lassen sich vor allem durch den Einsatz der elektronischen Signatur und separater Zeitstempel gut erfüllen. Vgl. für die Aktenführung bei E-Mail-Kommunikation auch oben S. 62.

Neben einer vollständigen elektronischen Aktenführung besteht eine weitere Möglichkeit in dem **Prinzip der doppelten Aktenführung**. Hier wird das eingehende Dokument sowohl digital, als auch ausgedruckt in Papierform zu den Akten genommen. Dies bietet sich insbesondere dort an, wo elektronische Dokumente aufgrund ihrer Bedeutung einer besonderen Sicherung bedürfen. Leicht führt dies allerdings zu dem Problem sog. **hybriden Akten**. Von solchen wird gesprochen, wenn sowohl ein papierbasiertes als auch ein elektronisches Vorgangsbearbeitungssystem genutzt wird und keine der beiden Ablageformen sämtliche Dokumente erfasst. Dem Grundsatz der Vollständigkeit wird in solchen Fällen nur dann entsprochen, wenn beide Systeme unter Berücksichtigung oben genannter Kriterien zusammengeführt werden können. Insbesondere ist daher über eine **eindeutige Kennzeichnung** entsprechender Verweise kenntlich zu machen, welche Dokumente des anderen Mediums jeweils einbezogen werden und wo sie zu finden sind.

6.4.8. Was ist aus datenschutzrechtlicher Sicht für eine elektronische Aktenführung beachtlich?

Hierzu führen die Datenschutzbeauftragten von Bund und Ländern folgendes aus: "Sind die Schriftstücke elektronisch abgelegt, ermöglichen elektronische Dokumentenverwaltungssysteme den schnellen, ungehinderten Online-Zugriff auf die Inhalte jedes einzelnen Dokumentes von jedem angeschlossenen Arbeitsplatz. Dabei kann das Wiederauffinden von

Dokumenten durch vielfältige Suchfunktionen unterstützt werden. Da die elektronischen Archivierungssysteme jedes Dokument gesondert erfassen, gehören Akten im klassischen Sinne (d.h. als physikalisch verbundene Dokumentensammlungen, die über ein einheitliches Kriterium - Aktenzeichen - erschlossen werden) der Vergangenheit an. Die "elektronische Bürgerakte" ist vielmehr rein virtuell, d.h. eine durch logische Zuordnungskriterien gebildete Datenzusammenstellung, wobei dasselbe Dokument zugleich Bestandteil verschiedener Akten sein kann. Es ist klar, dass diese übergreifenden Zuordnungs- und Auswertungsmöglichkeiten erhebliche Auswirkungen auf den Datenschutz haben."
Aus der Besonderheit dieser Situation ergeben sich folgende Handlungsempfehlungen der Bundes- und Landesdatenschutzbeauftragten:

- „Personenbezogene Daten dürfen nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Datenbestand, etwa in einer elektronischen Sachakte, muss daher zum frühest möglichen Zeitpunkt gelöscht oder zumindest gesperrt werden, wenn der ursprüngliche Verwendungszweck der Speicherung erfüllt ist.
- Gestaltung und Auswahl von Dokumentmanagement-Systemen haben sich an dem Ziel auszurichten, bei der Speicherung, Nutzung und Protokollierung so wenig personenbezogene Daten wie möglich zu verarbeiten.
- Auswertungen mit Data-Mining-Instrumenten sind grundsätzlich nur anonym oder pseudonym zulässig (Gefahr von Profilbildung).
- Betroffene sind umfassend zu unterrichten, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern" rechtswidrig.
- Für die Betriebssystemebene und für die Anwendung sowie für die Auswertung und die Statistiken des Datenbestandes ist ein Berechtigungs- und Zugriffskonzept festzulegen.
- Protokollierungen und Kontrollen sind festzulegen.
- Anforderungen an die Speicherung und die langfristige Aufbewahrung elektronischer Dokumente sind festzulegen.
- Der Einsatz einer elektronischen Signatur und die Verschlüsselung der gespeicherten Daten sind in Abhängigkeit des Schutzbedarfs vorzusehen.
- Eingangs- und Ausgangsschnittstellen zu anderen Verfahren sind inhaltlich und technisch zu dokumentieren.
- Ein Sicherheitskonzept und eine Dienstanweisung sollten erstellt werden."

Wie erfolgt eine Langzeitsicherung von elektronischen Verwaltungsakten?

Die Langzeitsicherung von elektronischen Verwaltungsakten hat zwei Komponenten: zum einen die Langzeitsicherung einer qualifizierten elektronischen Signatur, wenn der elektronische Verwaltungsakt aufgrund eines gesetzlichen Schriftformerfordernisses diese erforderte und zum anderen die Aufbewahrung bzw. Archivierung des elektronischen Dokuments. Diese Fragen der Langzeitsicherung sind nicht im SigG oder der SigV geregelt. Diese stellen lediglich Anforderungen an den Zertifizierungsdiensteanbieter hinsichtlich der zu gewährleistenden Dauer der Überprüfbarkeit von qualifizierten und akkreditierten elektronischen Signaturenzertifikaten.
Die Notwendigkeit der langzeitigen Aufbewahrung und Sicherung auch elektronischer Dokumente ergibt sich aber aus den **Aufbewahrungsfristen der jeweiligen Aktenordnungen** bzw. Aktenplänen innerhalb der Verwaltung. Die Aktenordnungen geben abhängig vom jeweiligen Schriftgut Aufbewahrungsfristen von bis zu 30 Jahren und im Einzelfall auch darüber hinaus vor, wobei z.B. für Schriftgut in Bundesministerien gem. § 19 Abs. 1 der Richtlinie für das Bearbeiten und Verwalten von Schriftgut Aufbewahrungsfristen von mehr als 30 Jahren auf den Ausnahmefall zu begrenzen sind. Im Rahmen der Aufbewahrung ist die **Vollständigkeit, Integrität, Authentizität und Lesbarkeit** des elektronisch gespeicherten Schriftguts durch geeignete Maßnahmen der Verwaltung zu gewährleisten (vgl. § 18 Abs. 1 S. 2 der Richtlinie). Eine geeignete Maßnahme ist das Signieren des Dokuments mit einer qualifizierten oder akkreditierten elektronischen Signatur und entsprechende Pflege des gespeicherten Schriftguts sowie ggf. eine erneute Signatur (vgl. unten S. 81). Laufen die Aufbewahrungsfristen der Aktenpläne für elektronisch gespeichertes Schriftgut ab, so ist dieses nach Vorgabe der Archivgesetze (ArchivG) des Bundes oder der Länder dem zuständigen Archiv zur weiteren Archivierung anzubieten.

Je zügiger eine – im Idealfall elektronische - Übermittlung des Schriftguts erfolgt, desto früher entfallen die weiteren Anforderungen an eine sichere Aufbewahrung des Dokuments innerhalb der Verwaltung.

Wie können elektronisch signierte Dokumente archiviert werden?

Ein mögliches Verfahren zur langfristigen Datensicherung von elektronisch signierten Dokumenten bietet § 17 SigV mit dem Modell des „**Übersignierens**". Vor dem Zeitpunkt des Ablauf der Eignung der Algorithmen oder der zugehörigen Parameter sind dem Verordnungswortlaut nach die "relevanten" Daten (siehe hierzu unten näher) erneut mit einer qualifizierten elektronischen Signatur zu versehen. Die erneute Signatur muss hierbei nicht nur mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, sondern auch die frühere Signatur mit einschließen und einen qualifizierten Zeitstempel tragen. Als rechtliche Folge des Übersignierens bleibt der gesetzliche Anschein der Echtheit des Dokuments gem. § 292a ZPO bestehen.
Zu beachten ist allerdings, dass das Übersignieren i.S.v. § 17 SigV lediglich den **Sicherheitszustand konserviert**, der durch die Ausgangssignatur begründet wurde. Eine darüber hinausgehende **dauerhafte Überprüfbarkeit der Signatur wird durch das Modell des Übersignierens nicht gewährleistet**. Das Übersignieren schützt also nur vor durch Technikentwicklungen eintretenden Unsicherheiten bei den verwendeten Algorithmen. Da keine Erweiterung der dauerhaften Überprüfbarkeit erfolgt, bleibt aus diesem Grund auch hier die Unterscheidung zwischen den unterschiedlichen gesetzlichen Anforderungen an die Überprüfbarkeit von qualifizierten oder akkreditierten elektronischen Signaturen beachtlich. Nur akkreditierte Signaturen ermöglichen eine dauerhafte Überprüfbarkeit des Zertifizierungspfades von mindestens 30 Jahren nach Ablauf des Zertifikats (vgl. hierzu oben S. 67). Zu den Anforderungen des § 17 SigV im Einzelnen:

- Die erneute Signatur muss **vor Ablauf der Eignung der Algorithmen oder zugehöriger Parameter** erfolgen. Die Veröffentlichung und Eignungsbestimmung der jeweiligen Algorithmen erfolgt nach Vorgabe der ersten Anlage zur SigV. Hiernach sind als geeignet i.S.d. SigV angesehene Algorithmen und zugehörige Parameter im Bundesanzeiger zu veröffentlichen. Ebenfalls wird der Zeitpunkt veröffentlicht, bis zu dem die Eignung jeweils gilt. Die Dauer der Eignung soll mindestens sechs Jahre ab Zeitpunkt der Bewertung und Veröffentlichung betragen. Werden also für das Erstellen einer elektronischen Signatur Algorithmen und zugehörige Parameter nach dem neuesten Stand der (aktuell veröffentlichten) Eignung verwendet, so kann davon ausgegangen werden, dass i.d.R. erst **nach frühestens sechs Jahren** übersigniert werden muss.
- **Übersignieren der relevanten Daten**: Es müssen nicht die archivierten Originaldaten erneut signiert werden; vielmehr wird dem Sicherheitsanspruch des § 17 SigV nach h.M. auch mit einem erneuten Signieren der Signatur-Hash-Werte der Ursprungssignatur entsprochen, da diese die jeweiligen Dokumente eindeutig abbilden. Werden die Hash-Werte der elektronischen Signaturen getrennt vom archivierten elektronischen Dokument gespeichert, kann hierdurch auch ein aufwendiger Zugriff auf die archivierten Originaldokumente vermieden werden. Vgl. zur Funktion der elektronischen Signatur bzw. des Hash-Wertes oben S. 66.
- **Keine Einzelsignatur nötig**. Letztlich muss nicht für jedes archivierte elektronische Dokument eine erneute singuläre elektronische Signatur oder ein entsprechender qualifizierter Zeitstempel erzeugt werden. Ausreichend für eine langfristige Datensicherung i.S.v. § 17 SigV ist auch das erneute Signieren vieler elektronischer Dokumente bzw. ihres Hash-Wertes mit nur einer qualifizierten elektronischen Signatur. Damit können auch größere Aktenbestände einfach übersigniert werden.

Wie erfolgt eine Langzeitsicherung elektronischer Signaturen?

§ 37 Abs. 4 VwVfG sieht vor, dass für Verwaltungsakte, die nach § 3a Abs. 2 VwVfG aufgrund eines gesetzlich bestimmten Schriftformerfordernisses einer qualifizierten elektronischen Signatur bedürfen, durch Rechtsvorschrift die dauerhafte Überprüfbarkeit vorgeschrieben werden kann. Hierdurch soll sichergestellt werden, dass Verwaltungsakte mit besonderer Bedeutung (z.B. **Dauerverwaltungsakte**) auch über längere Zeit beweiskräftig bleiben. Ausdrücklich normiert wurde dieses Erfordernis z.B. bereits in § 33 Abs. 5 Nr. 2 VwVfG für elektronische Beglaubigungen und gem. § 69 Abs. 2 S. 2 VwVfG für elektronische Verwaltungsakte bei Abschluss eines förmlichen Verwaltungsverfahrens i.S.v. § 63 Abs. 1 VwVfG. Der Umfang einer **dauerhaften Überprüfbarkeit der elektronischen Signatur** bestimmt sich

hierbei nach dem **Stand der Technik**. Ein qualifiziertes Zertifikat einer elektronischen Signatur gilt zur Zeit als dauerhaft überprüfbar, wenn der Zertifizierungsdiensteanbieter durch Organisation seiner technischen Infrastruktur sicherstellt, dass die von ihm ausgestellten qualifizierten Zertifikate für den im jeweiligen Zertifikat angegeben Gültigkeitszeitraum, sowie **mindestens 30 Jahre** über diesen Zeitraum hinausgehend, in einem sicheren Verzeichnis geführt werden. Grundlage einer dauerhaften Überprüfbarkeit, vor allem von Integrität und Authentizität des elektronischen Dokuments, ist daher die langfristige Aufbewahrung der Dokumentation durch einen Zertifizierungsdiensteanbieter. Diese Anforderungen erfüllt das Zertifikat einer qualifizierten elektronischen Signatur eines akkreditierten Zertifizierungsdiensteanbieters gem. § 15 SigG i.V.m. § 4 Abs. 2 SigV (vgl. oben S. 67).

Weiterführende Literatur: Zu Zeitstempeln: *Roßnagel* in Roßnagel (Hrsg.) Recht der Multimedia-Dienste, Loseblattkommentar, Stand Nov. 2000, SigG § 2 Rnr. 75ff; zum Problem der Langzeitsicherung qualifizierter elektronischer Signaturen, *Brandner/Pordesch/Roßnagel/Schachermayer*, DuD 26 (2002), S. 97ff. Zu Fragen der Archivierung *Wettengel* (Hrsg.), Digitale Herausforderung für Archive, Koblenz 1999, *Staatliche Archive Bayerns* (Hrsg.), Digitale Unterlagen – Entstehung/Pflege/Archivierung, München 2001; *KGSt*, Schriftgutverwaltung auf dem Weg zum digitalen Dokument, Bericht 3/2002; zur elektronischen Aktenführung *Roßnagel/Schroeder*, Multimedia in immissionsschutzrechtlichen Genehmigungsverfahren, 1999, S. 131ff.; *Idecke-Lux*, Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz, 2000, S. 91ff.; *Roßnagel,* Die digitale Signatur in der öffentlichen Verwaltung, in: Kubicek u.a. (Hrsg.), Multimedia@Verwaltung, Heidelberg 1999, S. 158ff. *Schreiber*, Elektronisches Verwalten. Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, 2002 S. 161 ff. Siehe insgesamt auch zu Fragen der Langzeitsicherung elektronisch signierter Dokumente die Grundsätze des Projektes "ArchiSig", Dez. 2002. Zur Notwendigkeit neuer Signaturen *Roßnagel/Hammer* in Roßnagel (Hrsg.) Recht der Multimedia-Dienste, Loseblattkommentar, Stand Nov. 2000, SigV § 18 Rnr. 20ff. Vgl. auch *Bundesministerium des Innern* (Hrsg.), Moderner Staat – Moderne Verwaltung, Registraturrichtlinien für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien, Beschluss des Bundeskabinetts v. 11. Juli 2001; zu Fragen des Datenschutzes im Bereich des Dokumentenmanagement LfD Niedersachsen(Hrsg.), „Datenschutzgerechtes eGovernment", Dezember 2002, S. 43f.

Abbildung 6: Elektronisches (Leistungs-)Verwaltungsverfahren

Verwaltung - Bürger

- **Elektronische Antragstellung**
  Grundvoraussetzung
  - Zugangseröffnung auf Behördenseite für elektronische Anträge gem. § 3 Abs. 1 VwVfG (vgl. 6.2.1)

↓

- **Form des Antrags**
  - ggf. elektronischer Formulargebrauch (vgl. 6.2.1)
  - ggf. qualifizierte elektronische Signatur (vgl. 6.3.3)

↓

- **elektronische Eingangsbestätigung**
  - z.B. mittels des Einsatzes elektronischer Zeitstempel im Posteingang der Verwaltung (vgl. 6.4.4)

Verwaltung

Elektronisches Bearbeiten des VwVf und elektronischer Erlass des VA

Elektronische Aktenführung: Anlegen einer elektronischen Akte zur Bearbeitung des Antrags im laufenden VwVf entsprechend den allgemeinen Grundsätzen aus § 29 VwVfG (vgl. hierzu unter 6.2.1 und 6.4.7)

↓

Form des elektronischen Verwaltungsaktes

↓ Grundsatz: **Formfreiheit**

VA kann gem. § 37 Abs. 2 S. 1 VwVfG
- schriftlich
- mündlich
- elektronisch (via E-Mail)
- oder auf andere Weise

erlassen werden.

↓ Ausnahme: **gesetzliches Schriftformerfordernis**

Gem. der Generalklausel des § 3 a Abs. 1 VwVfG erfolgt nur mit *qualifizierter elektronischer Signatur eine Gleichstellung der elektronischen zur Schriftform.*
Ausnahme: Gesetzlich angeordnetes Erfordernis der *dauerhaften Überprüfbarkeit* i.S.v. § 37 Abs. 4 VwVfG. Diese ist z.Z. nur durch eine akkreditierte elektronische Signatur i.S.v. § 15 SigG gewährleistet.

Signieren von Dokumentenanhängen: Auch hierfür besteht das Erfordernis der elektronischen Signatur, wenn die Anhänge aufgrund ihrer inhaltlichen Bedeutung faktischer Teil des VA werden.

↓

Elektronische Begründung des VA:
Erfordernis einer qualifizierten elektronischen Signatur für eine elektronische Begründung i.S.v. § 39 Abs. 1 S. 1 VwVfG nur, wenn der VA selbst einem Schriftformerfordernis unterliegt.

Verwaltung

- **Elektronische Langzeitsicherung von elektronischen VA**
  - entsprechend den jeweiligen Aktenplänen / Aktenordnungen
  - dauerhaften Sicherung elektronischer Dokumente durch Einsatz der elektronischen Signatur, ggf. Übersignieren gem. § 17 SigV (vgl. 6.4.9)

↓

- **Elektronische Übermittlung** relevanter Dokumente an die staatlichen Archive nach Vorgabe des jeweiligen ArchivG (vgl. 6.4.9)

Bürger

Zugangseröffnung auf Bürgerseite
Auch auf Seiten des Bürgers ist die Zugangseröffnung gem. § 3a Abs. 1 VwVfG Grundvoraussetzung für die elektronische Abwicklung eines Verwaltungsverfahrens (siehe hierzu unter 6.2.1)

↓

Elektronischer Zugang / Bekanntmachung
Entsprechend der Regelung in § 41 Abs. 2 VwVfG auch hier 3-Tages-Fiktion

↓

Elektronische Bestätigung formaler VA
- Mündlich erlassene VA können gem. § 37 Abs. 2 VwVfG auch elektronisch bestätigt werden. Das Erfordernis einer qualifizierten elektronischen Signatur besteht nicht.
- Formlos erlassene elektronische VA müssen schriftlich bestätigt werden. § 3a Abs. 2 VwVfG findet keine Anwendung.

6.5. Welche rechtlichen Probleme können bzgl. des Zugangs zu Online-Transaktionsangeboten der Verwaltung auftreten?

6.5.1. Muss die Verwaltung alle Signaturen akzeptieren?

Die Regelungen des SigG und der SigV erfassen im Kern nur die Anforderungen an qualifizierte elektronische Signaturen. Gem. § 1 Abs. 2 SigG ist daher die Verwendung sonstiger elektronischer Signaturen freigestellt, soweit nicht eine bestimmte elektronische Signatur durch Rechtsvorschrift vorgeschrieben ist. Eine Verwendung solcher Signaturen erfolgt dann auf der **Basis freiwilliger Vereinbarungen**. Dies bedeutet im Umkehrschluss, dass die Verwaltung in solchen Fällen, in denen keine Rechtsvorschrift eine qualifizierte elektronische Signatur erfordert, eine einfache elektronische Signatur akzeptieren kann, dies jedoch nicht muss. Eine Pflicht zur Akzeptanz aller Formen von Signaturen besteht für die Verwaltung demnach nicht. Die Pflicht zur Annahme besteht nur dann, wenn ein elektronisches Dokument mit einer zumindest qualifizierten elektronischen Signatur unterzeichnet wurde, eine gesetzliche Gleichstellung zur Schriftform besteht (§ 126a BGB/§ 3a Abs. 2 VwVfG) und die Übermittlung elektronischer Dokumente zulässig ist, da der Zugang durch die Verwaltung eröffnet wurde (§ 3a Abs. 1 VwVfG).

6.5.2. Welche technischen Vorgaben darf die Verwaltung für Signaturen treffen?

Aus § 3a Abs. 3 S. 2 VwVfG folgt die implizite Ermächtigung der Verwaltung zur Festlegung von Standards (siehe oben). Für die formgebundene Kommunikation und Transaktion ist im Rahmen dieser Ermächtigung daher auch die Festlegung der Verwaltung auf einen oder mehrere Anbieter von Signaturen innerhalb der Bestimmung technischer Rahmenbedingungen gem. § 3a Abs. 3 VwVfG zulässig, solange noch keine Interoperabilität zwischen Signaturverfahren unterschiedlicher Anbieter besteht. Um allerdings dem Bürger einen umfassenden Selbstschutz zu ermöglichen, sollte die Verwaltung immer auch akkreditierte Signaturen akzeptieren. Legt sich die Verwaltung auf einige Anbieter von Signaturen fest, so sollten daher immer auch akkreditierte Zertifizierungsdiensteanbieter i.S.v. § 15 SigG darunter sein. Eine Beschränkung auf nationale Anbieter wäre allerdings aufgrund europarechtlicher Vorgaben unzulässig.

6.5.3. Darf die Verwaltung vom Bürger ein höheres Signaturniveau als gesetzlich gefordert verlangen ?

§ 3a Abs. 2 VwVfG geht in seiner Funktion als Generalklausel von der Notwendigkeit einer qualifizierten elektronischen Signatur aus, wenn auf elektronischem Weg einem gesetzlichen Schriftformerfordernis entsprochen werden soll. Hieraus folgt, dass die Verwaltung ohne gesetzliche Grundlage weder zugunsten eines niedrigeren Sicherheitsniveaus von den Vorgaben des § 3a Abs. 2 VwVfG abweichen darf, noch höhere Ansprüche an die Signaturerfordernisse bei elektronischer Kommunikation stellen kann. Auch eine Beschränkung auf elektronische Signaturen nationaler Anbieter ist für die Verwaltung grds. unzulässig (vgl. hierzu unten).

6.5.4. Darf die Verwaltung ein höheres Signaturniveau verwenden?

§ 3a Abs. 2 VwVfG und spezialgesetzliche Vorgaben legen grundsätzlich auch für die Verwaltung das jeweils anzuwendende Signaturniveau fest. Nach unten darf die Verwaltung hiervon nie abweichen. Solange für den Bürger hierdurch keine Belastung ensteht, darf die Verwaltung jedoch freiwillig ein höheres als das gesetzliche Maß an Sicherheit bei der Verwendung elektronischer Signaturen wählen und z.B. ausschließlich elektronische Signaturen von akkreditierten Zertifizierungsdiensten verwenden. Zur Zeit sind alle deutschen Anbieter von qualifizierten Signaturverfahren i.S.d. SigG akkreditiert.

6.5.5. Muss die Verwaltung auch elektronische Signaturen ausländischer Zertifizierungsdiensteanbieter akzeptieren?

Für elektronische Signaturen aus dem Ausland gilt zunächst ebenso wie für inländische Signaturen § 1 Abs. 2 SigG. Soweit nicht eine bestimmte elektronische Signatur durch Rechtsvorschrift vorgeschrieben ist, ist ihre **Verwendung freigestellt**. Die Frage einer Pflicht zur Anerkennung be-

trifft daher Anwendungsfälle, in denen mit elektronischer Signatur Schriftformerfordernissen der Verwaltung entsprochen werden soll. § 23 SigG bestimmt die Anerkenntnis ausländischer elektronischer Signaturen und Produkte für elektronische Signaturen in **drei Fällen**. Sind diese gesetzlichen Anforderungen erfüllt, folgt hieraus auch eine Pflicht der Verwaltung zur Anerkennung. Dies allerdings nur, wenn aufgrund entsprechender Gesetze (§ 126a BGB / § 3a VwVfG) auch eine Pflicht zur Anerkennung (nationaler) qualifizierter elektronischer Signaturen besteht.

- Im ersten Fall erfolgt eine **generelle Anerkennung von elektronischen Signaturen** eines Zertifizierungsdiensteanbieters aus einem anderen Mitgliedstaat der EU oder des EWR, wenn dieser die Anforderungen des Art. 5 Abs. 1 Signatur-Richtlinie (Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. EG 2000 Nr. L 13 S.2) erfüllt (§ 23 Abs. 1 SigG). Sie werden qualifizierten elektronischen Signaturen i.S.d. SigG gleichgestellt, so dass auch mit ihnen den gesetzlichen Schriftformerfordernissen in Deutschland entsprochen werden kann.
- Im zweiten Fall sollen **Signaturen aus Drittstaaten** qualifizierten elektronischen Signaturen gleichgestellt werden, wenn das Zertifikat von einem dortigen Zertifizierungsdiensteanbieter öffentlich als qualifiziertes Zertifikat ausgestellt und für eine elektronische Signatur i.S.d. Art. 5 Abs. 1 Signatur-RL bestimmt ist und zusätzlich eine der in § 23 Abs. 1 Nr. 1-3 SigG beschriebenen weiteren Voraussetzungen erfüllt ist: gem. § 23 Abs. 1 Nr. 1 SigG hat sich der Zertifizierungsdiensteanbieter dem freiwilligen Akkreditierungssystem eines EU- oder EWR–Mitgliedstaates unterworfen; ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen der Richtlinie erfüllt, steht für das Zertifikat seines ausländischen Partners ein, oder das Zertifikat ist im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der EU und Drittstaaten oder internationalen Organisationen anerkannt.
- Im dritten Fall erfolgt gem. § 23 Abs. 2 SigG eine Gleichstellung ausländischer elektronischer Signaturen mit Anbieter-Akkreditierung nach § 15 Abs. 1 SigG, wenn sie nachweislich eine gleichwertige Sicherheit aufweisen.

6.5.6. Welche rechtlichen Konsequenzen ergeben sich durch eine fehlgeschlagene Signaturprüfung?

Besteht ein Schriftformerfordernis und bestimmt dieses für die elektronische Kommunikation zwingend die Verwendung einer qualifizierten elektronischen Signatur, finden bei einer fehlgeschlagenen Signaturprüfung die **allgemeinen Vorschriften des VwVfG zu Formfehlern** Anwendung. Denn ergibt die Signaturprüfung, dass es sich um eine fehlerhafte Signatur handelt, so ist der Antrag eines Bürgers oder der Verwaltungsakt der Verwaltung so zu behandeln, als wären sie ohne Signatur erstellt worden.
Ein **formwidriger Antrag ist im förmlichen Verfahren immer und im nicht-förmlichen i.d.R. unwirksam**. § 45 Abs. 1 Nr. 1 VwVfG lässt zwar die Nachholung eines formgerechten Antrags zu, Fristversäumnisse werden hierdurch aber nicht geheilt. Ist die Signaturprüfung fehlerhaft, so hat der Bürger daher erneut einen Antrag unter Verwendung einer funktionsfähigen Signatur zu stellen. Die Behörde muss regelmäßig den Antragsteller auf die Unrichtigkeit des Antrags und das Erfordernis eines neuen Antrags hinweisen.
Erlässt die Behörde einen formgebundenen Verwaltungsakt elektronisch und damit unter Verwendung einer elektronischen Signatur, so finden auch hier bei einer fehlgeschlagenen Signaturprüfung die allgemeinen Vorschriften über Formfehler Anwendung. Kann aufgrund der fehlerhaften Signatur die erlassende Behörde nicht erkannt werden, so hat dies gem. § 44 Abs. 2 Nr. 1 VwVfG die **Nichtigkeit des elektronischen Verwaltungsaktes** zur Folge. Ansonsten richten sich die Folgen nach dem **Einzelfall** und können von der Unbeachtlichkeit des Formverstoßes bis zur Nichtigkeit reichen. Der elektronische Verwaltungsakt ist hierbei so zu behandeln, als wäre er unter Nichtbeachtung der Formvorschrift erlassen worden.

6.5.7. Ist der Aussteller eines elektronischen Dokuments eindeutig zu identifizieren?

Bei einer elektronischen Unterschrift hat die Behörde Zugriff auf die Daten des dazugehörigen Zertifikats. Gem. § 7 Abs. 1 Nr. 1 SigG enthält ein qualifiziertes Zertifikat i.d.R. den **Namen des Signaturschlüssel-Inhabers**. Die Namensangabe gem. § 7 Abs. 1 Nr. 1 SigG bleibt jedoch im Umfang hinter den relevanten Angaben zurück, mit denen die Verwaltung i.d.R. eine Identifizierung vornimmt, wenn

hierfür eine gesetzliche Verpflichtung besteht. Eine Uneindeutigkeit besteht z.B. regelmäßig bei Namensgleichheit. Es ist allerdings zu beachten, dass in den meisten Fällen durch den Kontext bereits eine einmalige Zuordnung möglich ist. Auch in der "Papierwelt" ist die Überprüfung der Unterschriften nur sehr selten notwendig.

Wie kann das Identifizierungsproblem bei Namensgleichheit gelöst werden?

Eine eindeutige Identifizierung ist in Fällen sog. Namensgleichheit auf (alleiniger) Grundlage einer elektronischen Signatur nicht möglich. Gem. § 7 Abs. 1 Nr. 1 SigG ist zwar die Namensangabe im Zertifikat im Falle einer Verwechslungsgefahr mit einem Zusatz zu versehen. Dies schützt jedoch lediglich die **Einmaligkeit der Signatur**, nicht jedoch die eindeutige Identifizierung des Signierenden durch den Empfänger des signierten Dokuments. Eine Möglichkeit, dies im Rahmen der Online-Kommunikation zu vermeiden, wäre die Aufnahme von spezifischen Namenszusätzen wie **Geburtstag und Geburtsort in ein Attributzertifikat**. Ein anderer Weg wäre die einmalige Registrierung der Signaturen bei der Verwaltung. Für beide Maßnahmen besteht jedoch **keine gesetzliche Verpflichtung für den Bürger**. Darüber hinaus sind sie zumindest als datenschutzrechtlich problematisch anzusehen. Zur Speicherung von Grunddaten bei der Verwaltung vgl. oben S. 50.

Die Verwaltung darf den elektronischen Zugang auch nur dann von solchen Zusatzanforderungen abhängig machen, wenn diese für die ordnungsgemäße Durchführung des Verfahrens unverzichtbar sind. Da im Verwaltungsverfahren die qualifizierte elektronische Signatur aber oftmals nur als Unterschriftenersatz, nicht jedoch als Identifizierungsmöglichkeit dient, sind Probleme der Identifizierung z.B. in Fällen der Namensgleichheit von geringerer praktischer Relevanz. Meistens dürfte es wie im Schriftverkehr genügen, die eindeutig identifizierenden Merkmale anzugeben und zu signieren.

Steht die Verwendung eines Pseudonyms der Identifizierung entgegen?

Eine selbständige eindeutige Identifizierung ist der Verwaltung auch dann nicht möglich, wenn der Signierende nicht mit seinem Namen, sondern mit **Pseudonym** unterzeichnet. Diese Möglichkeit eröffnet § 7 Abs. 1 Nr. 1 SigG. Allerdings bestimmt § 3a Abs. 2 Satz 3 VwVfG für die elektronische Verwaltungskommunikation, dass die **Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüssel-Inhabers nicht ermöglicht, unzulässig ist**. Der Vorgang der Identifizierung muss dem Empfänger selbst möglich sein. Zumeist ist für den Bürger das Signieren mit Pseudonym in der Verwaltungskommunikation daher ausgeschlossen. Selbst wenn mit Pseudonym signiert wird, ohne dass die Behörde unmittelbar selbst den Unterzeichnenden identifizieren kann, bleibt zwar im Einzelfall eine Identifizierung der hinter dem Pseudonym stehenden Person über den Zertifizierungdiensteanbieter möglich. Denn auch das Pseudonym muss unverwechselbar und einer Person fest zugeordnet sein. Der Zertifizierungdiensteanbieter hat gem. § 5 Abs. 1 Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren und dies zu dokumentieren. Gem. § 14 Abs. 2 SigG sind sie aber nur verpflichtet, die Identität des Signaturschlüssel-Inhabers unter bestimmten Voraussetzungen z.B. zur Abwehr von Gefahren für öffentliche Sicherheit und Ordnung im Rahmen des Polizei- und Ordnungsrechts der Länder offen zu legen. Ein genereller Auskunftsanspruch gegenüber dem Zertifizierungsdiensteanbieter besteht nicht.

Für die Verwaltung schließt der Wortlaut des § 3a Abs. 2 S. 3 VwVfG die Verwendung eines Pseudonyms ebenfalls regelmäßig aus. Jedenfalls in den Fällen, in denen eine persönliche Unterschrift des Amtswalters aber grundsätzlich nicht erforderlich ist, kann jedoch von der Zulässigkeit der Verwendung eines Pseudonyms ausgegangen werden (insb. bei Empfangsbestätigungen, Verwaltungsakten). Die Verwaltung kann in solchen Fällen auch mit Pseudonym signieren, solange die handelnde Behörde und das zuständige Dezernat zu erkennen sind.

Weiterführende Literatur:
Zur Anerkennung ausländischer elektronischer Signaturen: *Roßnagel*, Das neue Recht elektronischer Signaturen, NJW 2002, S. 1817 (1824f). Zur Verwendung von Pseudonymen: *Roßnagel* in Roßnagel (Hrsg.), Multimedia-Recht, Loseblattkommentar, Stand Nov. 2000, SigG § 7 Rnr. 34ff. Zu dem Problem der vollständigen Identifizierung: *Roßnagel*, Der elektronische Ausweis, DuD 2002, S. 281ff.

6.6. Was ist bei der Elektronischen Vergabe zu beachten?

Die elektronische Vergabe bildet einen Sonderfall der elektronischen Transaktionen und kann hier nicht detailliert dargestellt werden. Die Vergabeverordnung und regelmäßig auch die Verdingungsordnungen eröffnen den Verwal-

tungen grundsätzlich die Möglichkeit, neben dem postalischen Weg auch ein elektronisches Vergabeverfahren durchzuführen. Die Zulassung elektronischer Angebote und die genaueren Bedingungen ihrer Abgabe sind in den Vergabeunterlagen anzugeben. Die Bekanntmachung der öffentlichen Ausschreibungen kann auch auf der Homepage erfolgen und die Vergabeunterlagen dürfen auch elektronisch bereitgestellt werden.

Für die besonders wichtigen öffentlichen Ausschreibungen gilt regelmäßig folgendes: Die elektronischen Angebote sind mit einer qualifizierten elektronischen Signatur zu signieren und zu verschlüsseln (vgl. nur § 15 VgV). Diese Angebote sind zu kennzeichnen (z.B. durch einen qualifizierten elektronischen Zeitstempel) und bis zum Eröffnungstermin ungeöffnet, also verschlüsselt, zu verwahren. Beim Eröffnungstermin stellt der Verhandlungsleiter die Unversehrtheit fest und entschlüsselt die Angebote. Der im Anschluss an die Bewertung erfolgende Zuschlag kann auch elektronisch mit qualifizierter elektronischer Signatur erfolgen, wenn der elektronische Zugang durch den Bieter eröffnet wurde.

Die allgemeinen Vergaberegeln erfordern für ein elektronisches Verfahren letztlich eine geeignete eigene Software. Eine solche hat etwa der Bund im Projekt E-Vergabe entwickelt und stellt sie den öffentlichen Verwaltungen zur Verfügung.

Weiterführende Literatur:
BMWi/BME (Hrsg.): Grundlagen der elektronischen Vergabe, 2002 (kostenloser download unter www.bme.de); Deutscher Städte- und Gemeindebund: E-Vergabe öffentlicher Aufträge, 2001.

6.7. Welche Modelle kommen für ein rechtskonformes Key-Management in Betracht?

Für eine medienbruchfreie elektronische Vorgangsbearbeitung ist auch die Übernahme klassischer Bearbeitungs- und Zeichnungsstrukturen in einen "elektronischen Workflow" notwendig. Sie lassen sich durch eine entsprechende Verteilung von Signaturen, Signaturkarten und Zertifikaten ("Key-Management") bedarfsgerecht nachbilden. Dabei sind die Funktion von Zeichnungsrechten sowie praktische Erwägungen wie die Berücksichtigung von Fachbereichswechseln und Mitarbeiterfluktuation unter Berücksichtigung der rechtlichen Anforderungen in die elektronische Vorgangsbearbeitung zu transformieren. Hierbei kann zwischen einzelnen Modellen des Key-Managements unterschieden werden, die in unterschiedlichem Maße den Anforderungen an Transparenz des Vorganges und Flexibilität der Zertifikatverteilung entsprechen.

- Ausreichende **Transparenz** erfordert zunächst die Möglichkeit für den Bürger zu erkennen, dass es sich bei dem übermittelten Dokument um eines der Verwaltung handelt. In der Regel erfordert dies jedoch nicht, dass der einzelne handelnde Beamte für den Bürger erkennbar wird. Auch das VwVfG stellt diese Anforderungen nicht einmal für den Erlass eines elektronischen Verwaltungsaktes. Wird mit einem elektronischen Verwaltungsakt einem Schriftformerfordernis entsprochen und er daher mit qualifizierter elektronischer Signatur versehen, muss gem. § 37 Abs. 3 S. 2 VwVfG das der Signatur zugrunde liegende qualifizierte Zertifikat oder ein zugehöriges Attributzertifikat lediglich **die erlassende Behörde** erkennen lassen. Gleichwohl gibt es Fälle, in denen es für den Bürger zur Wahrnehmung seiner Rechte erforderlich ist, die konkrete Identität des handelnden Beamten zu erfahren. So ist für Befangenheitsanträge i.S.v. § 21 VwVfG entscheidend, welcher konkrete Amtsträger gehandelt hat. Daher ist durch entsprechende Key-Management-Systeme oder Workflow-Strukturen zumindest die nachträgliche Identifizierbarkeit des konkret handelnden Beamten sicherzustellen.
- Ausreichende **Flexibilität und Praktikabilität** sind weitere wichtige Kriterien des Key-Managements. Für eine funktionsgerechte Organisation der Schlüsselvergabe ist z.B. die Berücksichtigung von Mitarbeiterfluktuation, Personalvertretungen und Zuständigkeitswechseln unabdingbar. Die Schlüsselstruktur sollte diesbezüglich flexibel gestaltet werden. Empfehlenswert ist z.B. die Möglichkeit, im Falle einer Vertretung andere Beamte unterzeichnen zu lassen, ohne die Formkonformität einerseits oder die Zeichnungsberechtigung andererseits zu verletzen. So wird aus organisatorischen und Kostengründen ein weites Einsatzspektrum der jeweils einem Bediensteten zugeordneten Signatur sinnvoll sein, um eine zu häufige Beantragung neuer Zertifikate und Schlüsselkarten vermeiden zu können.

6.7.1. Die Verwendung von personenbezogenen Hauptzertifikaten mit Namen des Schlüsselinhabers

Eine Möglichkeit den grundsätzlichen Anforderungen der Transparenz bei Einsatz der elektronischen Signatur gerecht zu werden, wäre eine Ausstattung der Verwaltungsbediensteten mit **individuellen Signaturkarten** und eine entsprechende Gestaltung des jeweiligen Zertifikatsinhalts. Das Signaturgesetz ermöglicht es, Eigenschaften des Signaturschlüsselinhabers und damit verwaltungsbezogene Angaben, in das Hauptzertifikat einzubringen, so dass bereits durch entsprechende Gestaltung des Signaturschlüsselzertifikats für entsprechende Tranzparenz gesorgt werden könnte. Zu beachten bleibt hierbei jedoch immer, dass je höher das Maß der individuellen Ausgestaltung des Hauptzertifikats ausfällt, die Wahrscheinlichkeit seiner Unrichtigkeit bei Änderung von Status oder Zeichnungsberechtigung der Bearbeiter bzw. Mitarbeiterfluktuation oder Fachwechsel zunimmt. Vgl. zu Vorgaben für den Inhalt von Zertifikaten und Folgen einer nachträglichen Unrichtigkeit oben unter S. 72.
Grundsätzlich wird ein Zertifikat daher umso flexibler auf Veränderungen reagieren können, je allgemeiner die Angaben im Schlüsselzertifikat sind. Letztlich erscheint daher lediglich der Hinweis auf die konkrete Behördenzugehörigkeit im Hauptzertifikat praktikabel. Aus rechtlicher Sicht ausreichend ist dies ebenfalls. Aus Datenschutzgesichtspunkten problematisch ist allerdings, dass auch im Falle der privaten Nutzung zwangsläufig die berufsspezifische Bezeichnung mit dem Hauptzertifikat versendet wird. In diesem Fall ist die private Nutzung ausgeschlossen, weil im Zertifikat immer angegeben ist, dass der Signierende für die Behörde handelt.

6.7.2. Das Modell der Verwendung von Attributzertifikaten

Eine Alternative zu Attributen in Signaturschlüsselzertifikaten stellt die Verwendung von Attributzertifikaten dar. Ein Attributzertifkat ist ein Signaturschlüssel-Zertifikat, welches weiterführende Angaben über den Schlüsselinhaber enthält, die nicht in das Hauptzertifikat eingetragen werden sollen. Die Möglichkeit, eine umfassende Transparenz zu erzeugen, ist durch die Verwendung eines Attributzertifikats ebenso hoch wie bei einem Hauptzertifikat, vorausgesetzt, dass es immer verwendet wird. Im Wesentlichen entspricht dieses Modell daher dem vorhergegangenen. Hinzu kommt allerdings, dass ein Attributzertifikat nur dann Teil der jeweiligen Signatur wird, wenn der Unterzeichnende dies will. Es besteht also eine **erhöhte Flexibilität** des Einsatzes der Signatur. Der Bedienstete könnte z.B. seine Standard-Signatur für den privaten Gebrauch nutzen und für den dienstlichen Einsatz die Signatur um ein Attributzertifikat mit den relevanten Behördenangaben ergänzen. Auch ist dieses Modell bei Veränderungen des Zertifikatsinhalts flexibler. Das SigG sieht nämlich keine Veränderung von Hauptzertifikaten vor, sondern lediglich ihre vollständige Sperrung. Eine Entsperrung ist für sie nicht möglich, so dass ein erneuter Antrag auf Erstellung einer Signaturkarte notwendig werden würde. Attributzertifikate sind dagegen austauschbar. Sie können gesperrt werden, ohne dass das Hauptzertifikat beeinträchtigt wird. Sollte es also zu einer Veränderung des Behördenstatus eines Beamten kommen, wäre lediglich das Attributzertifikat zu sperren und ein neues, aktualisiertes Attributzertifikat an das noch gültige Hauptzertifikat anzubinden.

6.7.3. Das Modell der pseudonymisierten aufgabenbezogenen Zertifikate

Das **Modell der pseudonymisierten aufgabenbezogenen Zertifikate** verwendet personenbezogene Hauptzertifikate, die aber nicht mit dem Namen des jeweiligen Signaturschlüsselinhabers, sondern mit einem Pseudonym versehen sind (z.B. Baubehörde der Stadt X). Die Verwendung eines Pseudonyms in einem qualifizierten Zertifikat ist gem. § 7 Abs. 1 Nr. 1 SigG zulässig. Zur Verwendung von Pseudonymen und den Grenzen im Verwaltungsverfahren siehe aber oben S. 86.
Das **aufgabenbezogene Zertifikat** beschreibt den jeweiligen Aufgabenbereich des zugeordneten Schlüsselinhabers und entspricht hierbei den grundsätzlichen Anforderungen der Transparenz. Die Zuweisung kann hier sogar **unabhängig von etwaigen Personenwechseln** bestehen bleiben, wenn sich bei Zuständigkeitswechseln u.ä. der neue zuständige Amtswalter gegenüber der Registrierungsstelle des Zertifizierungsdiensteanbieters neu identifiziert und seine Daten die des Vorgängers bei der Verknüpfung mit dem pseudonymisierten Zertifikat in den Dokumentationen ablösen. Anders als bei einem singulären Signaturschlüsselzertifikat oder einem Attributzertifikat ist hier eine Sperrung des Hauptzertifikats und anschließende Beantragung

einer neuen Signaturkarte bzw. Sperrung eines Attributzertifikats und Beantragung eines neuen bei Wechsel oder Ausscheiden von Bediensteten nicht notwendig. Da das SigG wohl nur von dem Verbot einer gleichzeitigen Mehrfachzuordnung eines Zertifikats zu mehreren Personen ausgeht, dürfte das Modell der pseudonymisierten aufgabenbezogenen Zertifikate auch gesetzeskonform sein. Eine endgültige Klärung steht allerdings noch aus.

6.7.4. Das Modell verwaltungseigener Signaturserver (Sicherheitsbox)

Ein weiteres Modell des Key-Managements stellt die Verwendung von verwaltungseigenen Signaturservern dar. Während die vorangegangenen Key-Management-Systeme zur Speicherung des privaten Schlüssels und des Zertifikats von einer chipkartenbasierten Lösung ausgingen, findet in diesem Modell ein **Kryptoprozessor** (Sicherheitsbox) Anwendung, welcher die Aufgaben der Chipkarte übernimmt (Authentisierung des Nutzers, Schlüsselerzeugung, Hashwertberechnung, Zertifikats und Signaturprüfung sowie Speicherung des öffentlichen Schlüssels). Hierdurch besteht die Möglichkeit der **Zentralisierung des Signiervorganges und die zügige Abwicklung von Massensignaturen**. So kann eine Sicherheitsbox z.B. in einer zentralen „elektronischen Poststelle" der Verwaltung eingesetzt werden, um mit einer signierten Erklärung den Eingang elektronischer Dokumente zu bestätigen. Der Einsatz einer Sicherheitsbox lässt es dabei technisch zu, dass ein einzelner Signaturschlüssel mit einem dazugehörigen Zertifikat verwendet werden kann, um alle der Signatureinheit zugeführten Dokumente mit einer elektronischen Signatur zu versehen. Allerdings bleibt auch dieses einzelne Zertifikat immer einer natürlichen Person zugeordnet, da es qualifizierte Zertifikate für Personenmehrheiten oder technische Einheiten nach dem deutschen SigG nicht gibt. Daneben besteht die Möglichkeit der Speicherung individueller Zertifikate und Schlüssel der Bediensteten, so dass auch die Erstellung von "eigenen" Signaturen durch die Bediensteten der Verwaltung möglich bleibt. Da es sich bei der Sicherheitsbox nur um eine andere Form der Signaturspeicherung handelt, gelten im Übrigen die vorangegangenen Ausführungen.

Für die rechtliche Zulässigkeit einer Sicherheitsbox ist zu beachten, dass das SigG gem. § 17 Abs. 1 SigG i.V.m. § 15 Abs. 1 SigV die alleinige Kontrolle des Signaturschlüssel-Inhabers über den Vorgang der Signierung fordert. Weiter muss die Sicherheitsbox den gesetzlichen Anforderungen sowohl für Signatureinheiten als auch Signaturanwendungskomponenten entsprechen.

Weiterführende Literatur:
Zum Key-Management umfangreich und detailliert: *Schreiber*, Elektronisches Verwalten: Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, 2002, S. 125-161.

6.8. Welche Anforderungen sind aus rechtlicher Sicht an die durch die Behörde eingesetzten Signaturkomponenten zu stellen?

Im einzelnen ergeben sich die technischen Anforderungen sowohl an sichere Signaturerstellungseinheiten als auch an Signaturanwendungskomponenten aus den §§ 17 und 15 Abs. 7 SigG. Eine Konkretisierung dieser Anforderungen erfolgt durch § 15 SigV. § 17 SigG stellt hierbei Anforderungen sowohl an Signaturkomponenten qualifizierter als auch akkreditierter elektronischer Signaturen, wobei die gesetzlichen Anforderungen allerdings unterschiedlich hoch ausfallen.

6.8.1. Welche Anforderungen bestehen für Signaturkomponenten qualifizierter Signaturen ?

Für technische Signaturkomponenten qualifizierter elektronischer Signaturen gilt gem. § 17 Abs. 4 S. 1 SigG, dass die Erfüllung der Anforderungen nach § 17 Abs. 1 und 3 Nr. 1 SigG durch eine anerkannte Stelle i.S.v. § 18 SigG **zu prüfen und zu bestätigen** ist. Zur Erfüllung der Anforderungen für technische Signaturkomponenten nach § 17 Abs. 2 und 3 Nr. 2 und 3 genügt dagegen eine bloße **Erklärung des Herstellers** darüber, dass den gesetzlichen Anforderungen entsprochen wird. Diese muss allerdings wohl auf einer geeigneten Prüfung aufbauen. Das zwingende gesetzliche Erfordernis einer Prüfung und Bestätigung durch eine anerkannte Prüf- und Bestätigungsstelle gem. § 18 SigG besteht für qualifizierte elektronische Signaturen also nur für Signaturerstellungseinheiten. Den weiteren Anforderungen des § 17 SigG sollen zwar auch Signaturanwendungskomponenten qualifizierter Signaturen entsprechen, zwingend ist dies allerdings nicht. Um einem möglichst hohen Maß an Sicherheit gerecht zu werden, wir allerdings grundsätzlich die Verwendung von **geprüften und bestätigten** Komponenten empfohlen.

6.8.2. Welche Anforderungen bestehen für Signaturkomponenten von akkreditierten Signaturen?

Dagegen besteht sowohl für Signaturerstellungs- als auch Signaturanwendungskomponenten akkreditierter Signaturen gem. § 15 Abs. 7 SigG die Notwendigkeit, die Erfüllung aller Pflichten aus § 17 Abs. 1-3 SigG geprüft und bestätigt bekommen zu haben. Die Anforderungen sind daher im Vergleich zu qualifizierten elektronischen Signaturen höher.

6.8.3. Muss das gesamte zu signierende Dokument am Bildschirm für den Signierenden sichtbar gemacht werden?

Gem. § 17 Abs. 2 S. 1 SigG sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, auf welche Daten sich die elektronische Signatur bezieht. Darüber hinaus müssen gem. § 17 Abs. 2 S. 3 SigG die Signaturanwendungskomponenten **bei Bedarf** auch den Inhalt der zu signierenden oder signierten Datei hinreichend erkennen lassen. Ziel der gesetzlichen Vorgaben ist es, dem Signierenden die Möglichkeit zu geben, nur solche Dateien zu signieren, die er auch optisch wahrgenommen und somit in seinen Entschluss zur Signierung mit einbezogen hat. Den Anforderungen des § 17 Abs. 2 S. 1 SigG kann aber bereits durch eine eindeutige Zuordnung der relevanten Datei zur Signatur erfüllt werden; die **vollständige Abbildung des Dokumenteninhalts auf dem Bildschirm ist hierfür nicht erforderlich**. Erweiterte Anforderungen bestehen allerdings durch § 17 Abs. 2 S. 3 SigG, da hier durch den Gesetzeswortlaut explizit auf die visuelle Wahrnehmung des Inhalts der zu signierenden Datei abgestellt wird. Allerdings ergibt sich auch aus § 17 Abs. 2 S. 3 SigG keine **absolute Verpflichtung zur Abbildung des zu signierenden Dokuments**. Einigkeit besteht nämlich zur Zeit darüber, dass teilweise die technische Realisierung der gesetzlichen Anforderungen zumindest bei komplexeren Dokumenten nicht möglich ist. Letztlich richten sich die Anforderungen aber ohnehin an den Hersteller von Signaturkomponenten. Der Verwaltung bleibt lediglich die Pflicht der sorgfältigen Auswahl gesetzeskonformer Signaturprodukte. Wählt sie geprüfte und bestätigte Signaturkomponenten, kann davon ausgegangen werden, dass sie ihren gesetzlichen Anforderungen entsprochen hat.

Weiterführende Literatur:
Zu Produkten nach SigG und die sog. Darstellungsproblematik: *Bovenschulte/Eifert*, Rechtsfragen der Anwendung technischer Produkte nach dem Signaturgesetz, DuD 26 (2002), S. 76ff.; *Pordesch*, Der fehlende Nachweis der Präsentation signierter Daten, DuD 2000, 89ff; *Schmidt*, Signiertes XML und das Präsentationsproblem, DuD 2000, 153ff.

6.9. Welche rechtlichen Probleme können durch das Angebot des E-Payments für die Verwaltung entstehen?

Ein integriertes Angebot des E-Payments für Verwaltungsdienstleistungen wirft zwei wesentliche rechtliche Fragen auf. Zum einen, ob sich die Verwaltung bei dem Angebot eines E-Payment-Verfahrens unterschiedlicher kommerzieller Anbieter bedienen darf und hierdurch den Bürger neben der allgemeinen Gebühr auch mit den Provisionsforderungen privater Kreditkarteninstitute belastet kann. Zum anderen, ob es die Grundsätze des Verwaltungsgebührenrechts zulassen würden, eine Nutzung der Online-Angebote im Rahmen der Gebührenbemessung durch niedrigere Gebühren zu honorieren oder umgekehrt den erhöhten Nutzen für den Bürger mit höheren Gebühren zu belegen. Schließlich stellt sich die Frage, ob die Verwaltung verpflichtet ist, anonyme Bezahlverfahren anzubieten.

6.9.1. Welche rechtlichen Anforderungen bestehen für die Nutzung der Kreditkarte als Online-Zahlungsmittel für Dienstleistungen der Verwaltung?

Der Anbieter von Kreditkartenzahlverfahren (in diesem Fall die Verwaltung) hat dem Kreditkartenunternehmen für jede erfolgte Transaktion einen bestimmten Prozentsatz der Transaktionssumme als Gegenleistung zu bezahlen (sog. **Disagio**). Mehrkosten treffen also in diesem Fall zunächst die Verwaltung. Es stellt sich daher die Frage, ob die durch Kreditkartenzahlung entstehenden Mehrkosten durch Anrechnung auf die Verwaltungsgebühr auf den Bürger abgewälzt werden können.
Einem solchen Aufschlag stehen zur Zeit zumindest die allgemeinen Geschäftsbedingungen (AGB) der einzelnen Kreditkartenunternehmen entgegen. Diese sehen in Form von sog. **Preisaufschlags-, Differenzierungs- bzw. Nichtdiskriminierungsklauseln** durchgängig ein Verbot kostenbedingter Zuschläge vor. Die öffentliche Verwaltung müsste also einen Vertrag mit Kreditkartenunternehmen ohne eine entsprechende Klausel aushandeln. Die Grund-

sätze des öffentlichen Rechts zur Gebührenerhebung (Äquivalenzprinzip, Kostendeckungsprinzip, Gebührengleichheit – vgl. hierzu nachfolgend die Ausführungen zur Gestaltung der Gebührensätze) stehen einer Differenzierung innerhalb der Gebührenbemessung zwischen Kreditkartenzahlung und sonstigen Zahlverfahren dagegen nicht entgegen. Das Kostendeckungsprinzip würde es allerdings auch zulassen, mittelbar die Transaktionskosten auf alle Nutzer der Dienstleistung umzulegen, so dass von einem individuellen Gebührenaufschlag für den einzelnen Nutzer abgesehen werden könnte.

6.9.2. Besteht die rechtliche Notwendigkeit anonymer Bezahlverfahren für Angebote der Verwaltung?

Um dem Grundsatz der vorbeugenden Datenvermeidung gerecht zu werden, fordern § 4 Abs. 6 TDDSG und § 13 Abs. 1 MDStV für Tele- und Mediendienste das Angebot anonymer oder pseudonymer Nutzungs- und Bezahlverfahren. Dies jedoch nur soweit, wie dies dem Diensteanbieter **technisch möglich und zumutbar** ist. Der Nutzer ist über ein solches Angebot zu informieren. Solange die Verwaltungsangebote ihrerseits keine Identifizierung des Kunden erfordern, sollte daher auch eine anonyme Zahlung der Verwaltungsgebühr online ermöglicht werden (z.B. mittels einer Geldkarte).

Weiterführende Literatur:
Zu Rechtsfragen datenschutzgerechter Online-Bezahlverfahren: *Grimm*, Elektronische Zahlungssysteme und Datenschutz, in: Horster/Fox (Hrsg.), Datenschutz und Datensicherheit, Braunschweig 1999; *Grimm*, Elektronische Zahlungssysteme im Überblick, in: Kubicek u.a. (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 2001, S. 197ff.; *Enzmann/Roßnagel*, Realisierter Datenschutz im elektronischen Einkaufen und Bezahlen – Das Projekt DASIT, CR 2002, S. 141ff.. Zur Schaffung anonymer oder pseudonymer Bezahlmöglichkeiten: *Schaar/Schulz*, in: Roßnagel (Hrsg.) Rechte der Multimedia-Dienste, Loseblattsammlung, Stand Nov. 2000, TDDSG, § 4, Rnr. 48 ff. Beispiele anonymer und datenschutzgerechter Zahlungssysteme: *LfD Niedersachsen* (Hrsg.), Datenschutzgerechtes eGovernment, Dez. 2002, S. 41ff.

6.10. Dürfen die Gebühren für Online-Verwaltungsdienste von den allgemeinen Gebührensätzen abweichen?

Eine Gebührendifferenzierung in Form einer Gebührenminimierung bei Nutzung elektronischer Verfahren kann Anreize für den Bürger schaffen, das Internet für die Abwicklung voll elektronischer Verwaltungsvorgänge zu nutzen. Die rechtliche Zulässigkeit einer Gebührendifferenzierung richtet sich nach den Vorgaben des allgemeinen Verwaltungsgebührenrechts.

- Das **Äquivalenzprinzip** stellt die gebührenrechtliche Ausprägung des Grundsatzes der Verhältnismäßigkeit dar. Es besagt, dass Gebühr und korrelierende Leistung derart in Beziehung zu setzen sind, dass durch die Bemessung kein Missverhältnis entsteht. Dabei wird die Leistung nach deren finanzieller Quantifizierung und nicht nach den Kosten der Leistungserstellung bewertet.
- Nach Vorgabe des **Kostendeckungsprinzips** dürfen Gebühren in der Regel höchstens so bemessen sein, dass die nach betriebswirtschaftlichen Grundsätzen ansatzfähigen Kosten der Verwaltungseinheit gedeckt werden. Die Summe der für die Leistungsart vereinnahmten Verwaltungsgebühr darf nicht über dem tatsächlichen Aufwand für die Erbringung der Leistung liegen. Das Prinzip der Kostendeckung steht jedoch unter dem Vorbehalt des Gesetzes, gilt also nur nach gesetzlicher Anordnung. Hierbei kann es als spezielles Kostendeckungsgebot, als Kostenüberschreitungsverbot oder auch als einfaches Kostenorientierungsgebot ausgestaltet sein.

Sowohl das Äquivalenzprinzip als auch das Kostendeckungsprinzip stehen einer Gebührendifferenzierung grundsätzlich nicht entgegen. Dem Kostendeckungsprinzip kommt vorrangig die Funktion eines Aufwandüberschreitungsverbots zu, das Äquivalenzprinzip legt lediglich einen Gebührenrahmen fest, in dem sich die Bemessung der Gebühr bewegen muss. Auch der **Gleichheitsgrundsatz** schränkt die Möglichkeit der Verwaltung zur Differenzierung der Gebühren nicht ein. Zwar ergeben sich auch aus Art. 3 Abs. 1 GG Vorgaben für die Gebührenberechnung (**Grundsatz der Abgabegerechtigkeit, Grundsatz der Gebührengleichheit**), die es zu beachten gilt. Es kann jedoch schon bezweifelt werden, ob überhaupt eine den Gleichheitssatz beeinträchtigende Belastung desjenigen besteht, der die relativ höheren Verwaltungsgebühren für die offline erbrachten Amtshandlungen zu leisten hat. Geht man von einer solchen Belastung aus, so liegt doch zumindest durch die **Anreizfunktion** zur Nutzung von Online-Angeboten der Verwaltung **ein sachlicher Grund für die Ungleichbehandlung** vor.
Im Ergebnis stehen der Verwaltung bei einer Gebührendifferenzierung also die allgemeinen Gebührengrundsätze

nicht entgegen. Zu berücksichtigen sind jedoch immer auch die einfachgesetzlichen Gebührenvorgaben für die einzelnen Verwaltungsdienstleistungen.

Weiterführende Literatur:
Zur Zulässigkeit der Gebührendifferenzierung: *Schreiber*, Elektronisches Verwalten: Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, 2002, S. 112ff.

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
Abschn.	Abschnitt
AfP	Archiv für Presserecht
AG	Amtsgericht / Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
Akz.	Aktenzeichen
Anm.	Anmerkung
ArchivG	Archivgesetz
Art.	Artikel
ASP	Application Service Providing
Auflg.	Auflage
AÜG	Arbeitnehmerüberlassungsgesetz
Ba-Wü	Baden-Württemberg
Bay	Bayern
BayBGG	Bayerisches Behindertengleichstellungsgesetz
BB	Betriebsberater
Bbg	Brandenburg
BBG	Bundesbeamtengesetz
Bd.	Band
BDSG	Bundesdatenschutzgesetz
bDSB	behördlicher Datenschutzbeauftragter
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGG	Behindertengleichstellungsgesetz
BGH	Bundesgerichtshof
BHO	Bundeshaushaltsordnung
BITV	Barrierefreie Informationstechnik-Verordnung
BMWA	Bundesministerium für Wirtschaft und Arbeit
BPersVG	Bundespersonalvertretungsgesetz
BRRG	Beamtenrechtsrahmengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVB-EDV	Besondere Vertragsbedingungen für die elektronische Datenverarbeitung
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise
CR	Computer und Recht
d.h.	das heißt
DA	Dienstanweisung
DENIC	Interessenverband Deutsches Network Information Center
ders.	derselbe
Difu	Deutsches Institut für Urbanistik
DÖV	Die öffentliche Verwaltung
Drittes VwVf-ÄndG	Drittes Verwaltungsverfahrensänderungsgesetz des Bundes
DuD	Zeitschrift für Datenschutz und Datensicherheit
DV	Datenverarbeitung
DVBl.	Deutsches Verwaltungsblatt
e.G.	eingetragene Genossenschaft
e.V.	eingetragener Verein
EG	Europäische Gemeinschaft
E-Government	Electronic Government
EigBG Ba-Wü	Eigenbetriebsgesetz Baden-Württemberg
E-Mail	Electronic Mail
E-Payment	Electronic Payment
EU	Europäische Union
EuGH	Europäischer Gerichtshof

EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
evt.	eventuell
EWG	Europäische Wirtschaftsgemeinschaft
f.	folgende
ff.	fortfolgende
gem.	gemäß
GemHVO	Gemeindehaushaltsverordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GkomZ	Gesetze der Länder über die kommunale Zusammenarbeit
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaft mit beschränkter Haftung
GO	Gemeindeordnung
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GWB	Gesetz gegen Wettbewerbsbeschränkungen
h.M.	herrschende Meinung
HABIT	Hagener Betrieb für Informationstechnologie
HGO	Hessische Gemeindeordnung
HGrG	Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder
Hrsg.	Herausgeber
i.d.R.	in der Regel
i.E.	im Erscheinen
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
ICANN	Internet Corporation for Assigned Names and Numbers
inkl.	inklusive
IT	Information Technologie
JurPC	JurPC – Zeitschrift für Rechtsinformatik
K&R	Kommunikation und Recht
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KG	Kammergericht (bei Gerichtsurteil)
KG	Kommanditgesellschaft
KGSt	Kommunale Gemeinschaftsstelle
KoopA/ADV	Koordinationsausschuss Automatische Datenverarbeitung Bund/Länder/Kommunen
KV M-V	Kommunalverfassung Mecklenburg-Vorpommern
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für Datenschutz
LG	Landgericht
LHO	Landeshaushaltsordnung
LSA	Land Sachsen-Anhalt
MarkenG	Markengesetz
MDStV	Mediendienstestaatsvertrag
M-V	Mecklenburg-Vorpommern
MMR	Multimedia & Recht
NGO	Niedersächsische Gemeindeordnung
NJW	Neue Juristische Wochenzeitung
Nov.	November
Nr.	Nummer
NW	Nordrhein-Westfalen
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht – Rechtsprechungsreport
NZBau	Neue Zeitschrift für Baurecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PC	Personal Computer
PersVG Bay	Bayrisches Personalvertretungsgesetz
PIN	Personenidentifikationsnummer
RegTP	Regulierungsbehörde Telekommunikation und Post
RDV	Recht der Datenverarbeitung

Rh-Pf	Rheinland-Pfalz
Rnr.	Randnummer
Rspr.	Rechtsprechung
s.o.	siehe oben
Saarl. KSVG	Kommunalselbstverwaltungsgesetz des Saarlandes
SächsGemO	Sächsische Gemeindeordnung
SGB IX	neuntes Sozialgesetzbuch
S-H	Schleswig-Holstein
Sig.-RL	Signaturrichtlinie
SigG	Signaturgesetz
SigV	Signaturverordnung
sog.	so genannte
StGB	Strafgesetzbuch
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdatenschutzverordnung
TKG	Telekommunikationsgesetz
TürKO	Thüringische Kommunalordnung
u.ä.	und ähnlichen
u.s.w.	und so weiter
UrhG	Urheberrechtsgesetz
Urt.	Urteil
UWG	Gesetz gegen den unlauteren Wettbewerb
v.a.	vor allem
VergabeR	Vergaberecht
VerwArch	Verwaltungsarchiv
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VgV	Vergabeverordnung
VK	Vergabekammer
VM	Verwaltung und Management
VOB	Verdingungsordnung für Bauleistungen
VOF	Verdingungsordnung für freiberufliche Leistungen
VOL/A	Verdingungsordnung für Leistungen – ausgenommen Bauleistungen Teil A
VwVfG	Verwaltungsverfahrensgesetz
VwGO	Verwaltungsgerichtsordnung
Web.-Dok.	Web-Dokument
WIPO	World Intellectual Property Organisation
WWW	World Wide Web
z.B.	zum Beispiel
z.Z.	zur Zeit
ZDA	Zertifizierungsdiensteanbieter
ZögU	Zeitschrift für öffentliche und gemeinwirtschaftliche Unternehmen
ZPO	Zivilprozessordnung

Stichwortverzeichnis

A

Abschlussfunktion 67
Abschottungs-Prinzip 49
Akkreditierte Signatur 68
  Anforderungen für Signaturkomponenten 90
Aktenführung 62
  datenschutzrechtliche Vorgaben 79
  elektronische Aktenführung im VwVf 79
  Gebot der Aktenmäßigkeit 62
  Gebot der Führung wahrheitgetreuer Akten 62
  Gebot der Vollständigkeit 62
  hybride Akten 79
  Prinzip der doppelten Aktenführung 79
Algorithmen 66
anonyme Bezahlverfahren 91
Anonymisierung 49
Application Service Providing 37
Äquivalenzprinzip 91
Archivierung 81
Attributzertifikat *Siehe* Zertifikat
Aufbewahrungsfristen 80
Auftragsdatenverarbeitung 35
ausländische Zertifizierungsdiensteanbieter 84
Auswahl privater Partner 25

B

Barrierefreie Informationstechnik-Verordnung 51
barrierefreie Zugänge zum Internet 52
Beglaubigungen 75
  Ausdrucke elektronischer Dokumente 75
  ehemaliger Papierdokumente 75
  von umformatierten Dokumenten 76
Beglaubigungsverbot 76
Behindertengleichstellungsgesetz 51
Benutzungsbedingungen 45
Betreibervertrag 30
  Regelungsaspekte 31
Betriebsrat 54
Betriebsvereinbarungen *Siehe* Dienstanweisungen
Beurkundungen 75
Beweiskraft elektronischer Signaturen 74
  Anscheinsbeweis 74
  Augenscheinbeweis 74
Branchenverzeichnis 17

C

Chatforen *Siehe* Diskussionsforen

D

Datenfriedhöfe 51
datenschutzgerechte Systemgestaltung 49
Datenschutzgrundsätze 45
  gesetzliche Grundlagen 45
Datenschutzhinweise 44
Datensparsamkeit 48
Datenvermeidung 48
dauerhafte Überprüfbarkeit 66
Deep-Link 58
DENIC e.G 12
Dienstanweisungen 53
  Beteiligung des behördlichen Datenschutzbeauftragten 54
  Beteiligung des Personal- oder Betriebsrates 53
  Regelungsaspekte 55
  über die Nutzung von E-Mail-Systemen 63
Dienstleistungskonzession 25
Diskussionsforen 63
  Ausschluss von Teilnehmern 65
  Haftungsprivilegierung 64
  Kontrollpflicht von Gästebüchern 64
  moderierte Diskussionsforen 64
  unmoderierte Diskussionsforen 64
Dispute-Eintrag 13
Domain 30
  als Sacheinlage 30
  Bemessung des Wertes 30
  Rückübertragung des Nutzungsrechts 30
Domaingrabbing 12
Domainrecht 12
  Anspruch auf Domain 12
  Behörden oder -teile 12
  ICANN-Schiedsverfahren 13
  Interessenabwägung 12
  Kennzeichnungscharakter 12
  Namensanmaßung 12
  Prioritätspronzip 12
  Schadensersatz 13
  Stadtnamen 12
  Top-Level-Domains ohne Landesbezug 13
  Verletzung des Namensrechts 13
  www.stadtname.de 12
  Zuordnungsverwirrung 12

E

Echtheitsfunktion 67
Eigenbetrieb 24
Eigengesellschaft 24
Eingangsbestätigung via E-Mail 78
Einwilligung 47
  elektronische Einwilligung 47
Einzelverträge über IT-Leistungen 37
  Regelungsaspekte 40
elektronische Signatur 66
  Abschlussfunktion 67
  Echtheitsfunktion 67
  Einmaligkeit der Signatur 86
  Festlegung von Signatuniveaus 84
  Funktionsäquivalenz 67
  Funktionsweise 66
  Garantiefunktion 67
  Identitätsfunktion 67
  Langzeitsicherung 81
  Perpetuierungsfunktion 67
  rechtliche Unterschiede 69
  Regelungsniveaus 67
  Signaturen aus Drittstaaten 85
  technische Vorgaben 84
  Warnfunktion 67

Entwicklungspartnerschaften 40
Regelungsaspekte 41
E-Payment 90
EVB-IT 39
Exklusivvereinbarungen 33

F

Formfreiheit 59
formwidriger Antrag 85
Frame-Link
Zustimmungserfordernis 58
Frame-Links 57
Funktionsübertragung 35

G

Garantiefunktion 67
Gebührendifferenzierung 91
Gemeinderatbeschluss 23
gemischtwirtschaftliche Unternehmen 24
Auswahl privater Partner 25
städtische Mitarbeiter 31
Generalklausel 66
Gesellschaftsvertrag 30
Regelungselemente 30
Gleichheitsgrundsatz 91
Gleichstellung von Behinderten 51
GmbH 30
Aufsichtsrat 30
GmbH&Co.KG 30
Grunddaten 50
Grundsatz der Wirtschaftlichkeit und Sparsamkeit 23

H

Haftung für Informationsinhalte 57
für eigene Informationen 57
für fremde Informationen 57
Haftung für rechtswidrige Inhalte in Hyperlinks 57
Haftungsgrundsätze *43*
eigene Inhalte 43
fremde Inhalte 43
Hash-Wert 66
Hyperlink 58
Zustimmungserfordernis 58

I

Identifikationsfunktion 67
Identifizierung 85
Impressumspflicht 43
Individualkommunikation 42
informationelle Gewaltenteilung 49
informationelle Selbstbestimmung 45
Informationsangebote 56
Bündelung regionaler Angebote 18
Daseinsvorsorge 17
datenschutzrechtliche Vorgaben 56
Hilfsbetrieb 16
öffentlicher Zweck 17
überregionale private Angebote 19
wirtschaftliche Betätigung 15
Zulässigkeit 15
Inhaltsdaten 49
Inhaltsebene 47
Inhaltskontrollen 54
Inhouse-Geschäft 25
Inline-Links 57
Interkommunale Zusammenarbeit 34
Intermediär 15
IT-Know How 37

K

Kennzeichenpflichten 43
einfache Anbieterkennzeichnung 43
qualifizierte Anbieterpflicht 43
Key-Management 87
Modell der Attributzertifikate 88
Modell der pseudonymisierten aufgabenbezogenen Zertifikate 88
Modell verwaltungseigener Signaturserver 89
Kommunales Wirtschaftsrecht 14
Bedarf 14
Beurteilungsspielraum 14
Leistungsfähigkeit der Gemeinde 14
öffentlicher Zweck 14
Subsidiaritätsklausel 14
UWG 15
Wirtschaftsklauseln 14
Zulässigkeit von Internetangeboten 14
Kommunikation via E-Mail 59
alternative Handlungsform 61
Einwilligung zur Online-Kommunikation 60
fehlerhafte elektronische Kommunikation 61
Informationspflicht 61
Pflicht zur Online-Kommunikation 60
technische Vorgaben 61
Zugangseröffnung 60
Kommunikationsangebote 59
meinungsbildende Relevanz 18
Zulässigkeit 18
Kontroll- und Einflusspflichten 30
Kreditkarte als Online-Zahlungsmittel 90
Kryptogramm 66
Kryptoprozessor 89

M

Marktplatz der Meinungen 63
materieller Aktenbegriff 62
Mediendienstestaatsvertrag 42
Mehrwertdienste 18
Subsidiaritätsklausel 19
Zulässigkeit 18
Musterdienstanweisung 63

N

Namensgleichheit 86
Namensrecht 12
Nutzungsbedingung
Regelungsaspekte 64
Nutzungsbedingungen 64
Einbeziehung 45
für Chat- und Diskussionsforen 64
Publizität 64
Nutzungsdaten 49

O

öffentliche Einrichtung 52
Nutzungsbedingungen einer 53
Nutzungsgrenzen 53
Qualifikation als öffentliche Einrichtung 53
Zulassungsanspruch 53
öffentlicher Zweck 14
Öffentlichkeitsarbeit 56
öffentlich-rechtlichen Organisationsform 24
Organisationsformen 21
Beurteilungsspielraum 23
Erfüllung der Aufgaben 23
Gemeinderatbeschluss 23
Grundsatz der Wirtschaftlichkeit und Sparsamkeit 23
interkommunale Zusammenarbeit 34

öffentlich-rechtliche Organisationsform 24
privater Betrieb 24, 32
Rechtmäßigkeitserwägungen 21
Wirtschaftlichkeitsuntersuchungen 23
Zweckmäßigkeitserwägungen 21
Outsourcing-Verträge
Regelungsaspekte 40

P

Perpetuierungsfunktion 67
personenbezogene Daten 47
Einwilligung des Betroffenen 47
Erhebung 47
gesetzliche Ermächtigung 47
Löschung 50
Sperrung 50
Verarbeitung 47
Verwendung von Bedienstetendaten 56
Pflichtenheft 39
Prioritätsprinzip 12
Private Nutzung 63
privatrechtliche Organisationsform 24
GmbH 24
GmbH&Co. KG 24
Projekt E-Vergabe 87
Protokollierung 54
Pseudonym 86
Pseudonymisierung 49

Q

Qualifizierte elektronische Signatur 67
Anforderung für Signaturkomponenten 89

R

Rahmenvertrag 38
Randnutzung 14
Rechtsbehelfsbelehrung 76
Regiebetrieb 24
Registrierungsstelle 20

S

Schlichtungsstelle 64
Schriftformerfordernis 60
Schwellenwert 26
SGB IX 52
Sicherheitsbox 89
Signaturkomponenten 89
Signaturrichtlinie 71
Software-Signaturen 73
standardisierte Vertragsbedingungen 39
Standards 63
Subsidiaritätsklausel 14

T

Technik- und arbeitsplatzbezogenen Vorschriften 53
technische Rahmenbedingungen 61
Teledienste
Zulassungsfreiheit 42
Teledienstedatenschutzgesetz 42
Teledienstegesetz 42
Transaktionsangebote 65, 84
Zulässigkeit 18

U

Übersignieren 81
urheberrechtlich geschützter Werke 59

V

Verbot des widersprüchlichen Verhaltens 65
Verein 32
Vergaberecht 25
Anwendung auf gemischtwirtschaftliche Betreiber 38
Anwendungsbereich 25
Ausnahmen 25
Bagatellbeschaffung 27
Dienstleistungskonzession 32
elektronische Vergabe 86
offene Verfahren 26
öffentliche Ausschreibung elektronisch 87
Projektanten 26
Schwellenwerte 26
Verdingungsverordnungen 37
Verfahren 26
Verhandlungsverfahren 27
Vorgaben 26
Verwaltungsakt 76
Begründung 78
Drei-Tages-Fiktion 78
elektronische Bestätigung 79
Grundsatz der Formfreiheit 76
Langzeitsicherung 80
Zugang 77
Zugangshindernisse 77
Verwaltungsrechtsverhältnis 61
virtuelle Poststelle 50
datenschutzrechtliche Vorgaben 50
Einrichtung von Postfächern 63
Regelung des Postausgangs 63
Regelung des Posteingangs 63
virtuelles Hausrechts 65
virtuelles Trustcenter 20

W

Warnfunktion 67
Werbung 19
Widmungsakt 52
wirtschaftliche Betätigung 14
Wirtschaftlichkeitsuntersuchungen 23
Wirtschaftsklauseln 14

Z

Zeitstempel 78
Zertifikat 72
Attributzertifikat 72
Beantragung 73
Hauptzertifikat 72
nachträgliche Unrichtigkeit 73
Sperrung 73
vorgeschriebener Inhalt 72
Zertifizierungsdiensteanbieter 20
öffentliche Stellen als 20
Zertifizierungsstelle
Anforderungen der Verwaltung 72
Rahmenverträge 71
Zugangseröffnung 60
Zweckbindung 48

Zu den Autoren

Dr. Martin Eifert LL.M. studierte Rechtswissenschaften in Hamburg, Genf und Berkeley. Er war vier Jahre wissenschaftlicher Mitarbeiter an der Universität Hamburg (Prof. Dr. Hoffmann-Riem) und arbeitete gut ein Jahr als Unternehmensberater bei The Boston Consulting Group. Seit 1999 ist er am Hans-Bredow-Institut mit der rechtswissenschaftlichen Begleitforschung des *MEDIA*@Komm-Projekts betraut. Er ist Habilitant des Fachbereichs Rechtswissenschaften der Universität Hamburg und Habilitationsstipendiant der Deutschen Forschungsgesellschaft. Das Habilitationsprojekt behandelt die „Rechtsstrukturen des Electronic Government".

Jan Ole Püschel studierte Rechtswissenschaften an der Universität Hamburg und am University College Cork in Irland mit dem Schwerpukt Information und Kommunikation. Von April 1999 bis Juli 2001 war er wissenschaftliche Hilfskraft von Prof. Dr. Ramsauer mit Schwerpunkt im Verwaltungs- und Verwaltungsverfahrensrecht. Seit August 2001 ist er wissenschaftlicher Mitarbeiter am Hans-Bredow-Institut und hier innerhalb der rechtswissenschaftlichen Begleitforschung zum *MEDIA*@Komm-Projekt tätig. Sein Promotionsvorhaben setzt sich mit rechtlichen Rahmenbedingungen einer kommerziellen Nutzung von Verwaltungsinformation auseinander.

Ass. jur. Claudia Stapel-Schulz studierte nach dem Vordiplom in Betriebswirtschaftslehre Rechtswissenschaften in Hamburg, Lausanne und Speyer. Sie war gut ein Jahr als Referentin im Medienreferat der Staatskanzlei des Landes Schleswig-Holstein mit den Schwerpunkten europäisches Medienrecht und Medienpolitik tätig. Im September 1999 wurde sie vom Landesdienst für ihre Tätigkeit am Hans-Bredow-Institut beurlaubt. Dort arbeitete sie von September 1999 bis Dezember 2002 in der rechtswissenschaftlichen Begleitforschung des Projektes *MEDIA*@Komm. In ihrer Dissertation bearbeitet sie das Thema „Zulässigkeit städtischer Internetauftritte".

Autorinnen und Autoren:
Martin Eifert
Jan Ole Püschel
Claudia Stapel-Schulz

Layout:
Barbara Geffe, Elke Postler, Berlin

Herausgeber:
Hans-Bredow-Institut
Heimhuder Straße 21
20148 Hamburg
Telefon: 040/450 217-0
www.hans-bredow-institut.de

Im Auftrag des Bundesministeriums für Wirtschaft und Arbeit

Alle Rechte vorbehalten

Februar 2003

ISBN 3-87296-100-4

Deutsches Institut für Urbanistik,
DIN Deutsches Institut für Normung e.V.,
Hans-Bredow-Institut für Medienforschung
in Verbindung mit der Forschungsstelle Recht
und Innovation an der Universität Hamburg,
TÜV Informationstechnik GmbH

Der Städtewettbewerb
Multimedia *MEDIA*@Komm
und die Begleitforschung
werden gefördert vom
Bundesministerium
für Wirtschaft und Arbeit

MEDIA@Komm

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit des Bundesministeriums für Wirtschaft und Technologie herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Europa-, Bundestags-, Landtags- und Kommunalwahlen. Missbräuchlich sind insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Bundesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.

ISBN 3-87296-100-4