



Universität Bremen, Technologie-Zentrum Informatik

Qualitätskriterien für einen bürgerfreundlichen und sicheren Web-Auftritt

Der hier vorliegende Text ist ein Modul aus dem

E-Government-Handbuch

<http://www.E-Government-handbuch.de>

Redaktion: Projektgruppe E-Government im
**Bundesamt für Sicherheit in der
Informationstechnik (BSI)**

Kontakt: egov@bsi.bund.de



Inhaltsverzeichnis

1	Einleitung und Überblick.....	6
1.1	Zielsetzung.....	6
1.2	Ausgangsszenario	7
1.2.1	Typischer konventioneller Ablauf eines Bürger-Behörde-Kontakts (Antragsverfahren).....	8
1.2.2	Voraussetzungen für die Nutzung von Online-Angeboten.....	8
1.2.3	Motivation des Bürgers für die Nutzung von Online-Dienstleistungen	9
1.2.4	Typischer Ablauf (online) eines Bürger-Behörde-Kontakts (Antragsverfahren).....	9
1.3	Qualitätskriterien	10
1.3.1	Zugang	10
1.3.2	Qualität von Inhalt und Funktionen.....	10
1.3.3	IT-Sicherheit	11
1.3.4	Datenschutz.....	12
1.3.5	Verantwortlichkeit für Inhalte	12
1.4	Prioritäten, Hilfe zur Bewertung.....	13
1.5	Checkliste	14
2	Zugang	15
2.1	(Technische) Zugänglichkeit und Auffindbarkeit.....	15
2.1.1	Auffindbarkeit im Internet.....	15
2.1.2	Kompatibilität.....	17
2.1.3	Performanz.....	21
2.2	(Inhaltliche) Erschließung.....	23
2.2.1	Allgemeine Orientierung	23
2.2.2	Suchmaschine	25
2.2.3	Mehrsprachigkeit	27
2.2.4	Barrierefreiheit.....	28
2.2.5	Navigation.....	30
2.2.6	Hilfen	31
3	Inhaltliche Angebote und Funktionen.....	33
3.1	Informationsangebote	33
3.1.1	Umfang und Tiefe.....	34
3.1.2	Anforderung von Informationsmaterial	37
3.1.3	Nutzungsqualität.....	38

3.2	Kommunikationsangebote	40
3.2.1	E-Mail	40
3.2.2	Newsletter	42
3.2.3	Mailinglisten	43
3.2.4	Diskussionsforen.....	44
3.2.5	Chat.....	46
3.3	Transaktionsangebote	46
3.3.1	Umfang und Tiefe.....	50
3.3.2	Payment	52
3.3.3	Nutzungsqualität	54
4	IT-Sicherheit	58
4.1	IT-Sicherheitsmanagement	59
4.2	Erklärungen der Behörde zur IT-Sicherheit.....	60
4.3	Aktive Inhalte	60
4.4	Kryptografie und Verbindungssicherheit, Authentisierung	61
4.5	Absicherung von Web-Servern per Firewall	62
4.6	Administration von Web-Servern.....	63
5	Datenschutz.....	65
5.1	Transparenz.....	65
5.1.1	Anbieter- bzw. Behördenkennzeichnung.....	65
5.1.2	Datenschutzerklärung/ Privacy Policy.....	66
5.1.3	Informationen über Weitervermittlung.....	69
5.2	Materielle Rechtmäßigkeit der Datenverarbeitung	69
5.2.1	Erhebung, Speicherung und Auswertung von Nutzungsdaten	69
5.2.2	Erhebung, Speicherung, Nutzung von Bestandsdaten	70
5.2.3	Einwilligung des Bürgers.....	71
5.2.4	Übermittlung von Bestands- und Nutzungsdaten an Dritte	72
5.2.5	Pseudonyme Auswertung von Bestands- und Nutzungsdaten.....	73
5.2.6	Speicherung und Löschung von E-Mails.....	74
5.2.7	Cookies, Web-Bugs und ähnliche nutzeridentifizierende Techniken.....	74
5.2.8	Wahrung der Rechte der betroffenen Bürger.....	76
5.3	Datensparsamkeit.....	77
6	Verantwortlichkeit für Inhalte	79
6.1	Verantwortlichkeit für eigene und fremde Inhalte.....	79
6.2	Jugendschutz.....	81

7	Mustertexte	83
8	Checklisten	92
8.1	Zugang (s. Kap. 2)	92
8.1.1	(Technische) Zugänglichkeit/ Auffindbarkeit (s. Kap. 2.1).....	92
8.2	(Inhaltliche) Erschließung (s. Kap. 2.2).....	93
8.2.1	Allgemeine Orientierung (s. Kap. 2.2.1)	93
8.3	Inhaltliche Angebote und Funktionen (s. Kap. 3).....	96
8.3.1	Informationsangebote (s. Kap. 3.1).....	96
8.3.2	Kommunikationsangebote (s. Kap. 3.2)	98
8.3.3	Transaktionsangebote (s. Kap. 3.3)	100
8.4	IT-Sicherheit (s. Kap. 4)	103
8.4.1	IT-Sicherheitsmanagement (s. Kap. 4.1)	103
8.4.2	Erklärungen der Behörde zur IT-Sicherheit (s. Kap. 4.2).....	103
8.4.3	Aktive Inhalte (s. Kap. 4.3).....	104
8.4.4	Kryptografie und Authentisierung (s. Kap. 4.4)	104
8.4.5	Absicherung von Web-Servern per Firewall (s. Kap. 4.5)	105
8.4.6	Administration von Web-Servern (s. Kap. 4.6).....	106
8.5	Datenschutz (s. Kap. 5).....	106
8.5.1	Transparenz (s. Kap. 5.1).....	106
8.5.2	Materielle Rechtmäßigkeit der Datenverarbeitung (s. Kap. 5.2)	108
8.5.3	Datensparsamkeit (s. Kap. 5.3).....	112
8.6	Verantwortlichkeit für Inhalte (s. Kap. 6).....	112
8.6.1	Verantwortlichkeit für eigene und fremde Inhalte (s. Kap. 6.1)	112
8.6.2	Jugendschutz (s. Kap. 6.2).....	112
9	Autorendarstellung	113

Informationen zum Modul

Status	Beitrag von datenschutz nord und tzi
Autor	Herr Dr. Martin Wind, Herr Uwe Schläger
Ansprechpartner/ Kontakt	Herr Rainer Belz (BSI), mailto:egov@bsi.bund.de

Änderungsverzeichnis

Datum	Name	Änderung
12.12.2002	Horn	Redaktionelle Überarbeitung/Einfügen Autorendarstellung
31.10.2002	Dr. Wind, Schläger	erste Version

Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urhebergesetzes ist ohne Zustimmung des Bundesamtes für Sicherheit in der Informationstechnik unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

© 2002

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn

1 Einleitung und Überblick

1.1 Zielsetzung

Das Bereitstellen von Informationen und Dienstleistungen im World Wide Web ist mit der Investition von Ressourcen und der Anwendung von Experten-Know-how verbunden. Die Höhe der eingesetzten Mittel allein gibt jedoch keinen Aufschluss über die erreichte Qualität eines Online-Angebots.

In der Wirtschaft und Industrie werden „schlechte“ Web-Angebote durch ausbleibendes Nachfrageverhalten quittiert, welches in der Regel zu schnellen Reaktionen der Unternehmen führt, um größeren Schaden zu vermeiden.

Im Gegensatz dazu hat der Bürger bei der Inanspruchnahme von Online-Dienstleistungen bei Behörden keine Wahlmöglichkeit; es existiert keine direkte Konkurrenz. Für eine Dienstleistung ist in der Regel genau eine Behörde zuständig, ohne Ausweichmöglichkeit. Die Behörde muss also selbst auf die Qualität ihres Angebots achten. Bisherige Methoden zur Qualitätssicherung (Qualitätsmanagement, Controlling) in der öffentlichen Verwaltung berücksichtigen die Qualität eines Web-Auftritts aus Bürgersicht jedoch kaum.

Zeitschriftenredaktionen, Unternehmensberatungen und Verbände führen so genannte Rankings oder Benchmarking-Vergleiche durch, die in der Regel dazu dienen, die „besten“ Angebote zu identifizieren. Die Kriterien und Bewertungsverfahren dieser Vergleiche variieren stark. Oft lassen sie auch nicht erkennen, was konkret getan werden sollte, um eine bessere Note zu erhalten.

Dieses Kapitel listet Anforderungen auf, die ein typischer Kunde an die Web-Inhalte einer Behörde berechtigterweise stellt. Hierbei sollen Kundenfreundlichkeit und IT-Sicherheit im Vordergrund stehen.

Zielgruppe des Moduls sind in erster Linie E-Government-Koordinatoren und IT-Verantwortliche in Bundesbehörden, aber auch in Landes- und Kommunalbehörden, die an der Realisierung von E-Government-Angeboten beteiligt sind.

Zielgruppen

Das Modul beschreibt Maßnahmen, mit denen diese einen Web-Auftritt bürgerfreundlich und sicher machen können. Durch eine schlichte Ja-nein-Abfrage in der erstellten Checkliste ist es möglich, den Status quo zu analysieren und umzusetzende Maßnahmen herauszuarbeiten. Auf eine quantitative Bewertung, Gewichtung und Zusammenfassung zu Schulnoten kann für diesen Zweck verzichtet werden.

Durch Anwendung der Checkliste und Umsetzung der Maßnahmen kann jede Behörde die Qualität ihres Online-Angebots nachhaltig erhöhen. Erwünschtes Ergebnis: Das angebotene Online-Verfahren bietet sowohl Bürgern als auch der Behörde Vorteile gegenüber der „klassischen“ Leistungserbringung.

1.2 Ausgangsszenario

Bei der Erarbeitung der Texte und Checklisten wurde von folgendem Szenario ausgegangen: Der Bürger hat die Absicht mit einer Behörde in Kontakt zu treten, um eine bestimmte Aktion durchzuführen. Der Bürger verfolgt diese „Aufgabe“ in der Regel eher selten. Wenn er sie bewältigt, geschieht es überwiegend nicht aus eigenem Antrieb, sondern um einer gesetzlichen Vorgabe Genüge zu tun. Beispiele für eine geplante Aktion sind: Rückzahlung BAföG, Einkommensteuererklärung, Beantragung Personalausweis.

Es muss davon ausgegangen werden (Worst-case-Szenario), dass der Bürger nicht genau weiß,

Worst-case-Szenario

- welche Behörde für seine Angelegenheit zuständig ist,
- wie der rechtliche Fachausdruck für die beabsichtigte Aktion lautet,
- ob er in der Lage ist, die beabsichtigte Aktion ohne weitere Hilfsmittel oder Formulare erledigen zu können,
- ob es sinnvoll oder notwendig ist, sich für die Erledigung der geplanten Aktion vorher durch Dritte beraten zu lassen.

Trotz dieses Unwissens möchte der Bürger die Aktion mit möglichst geringem Ressourceneinsatz bewältigen. Die bestimmenden Ressourcen sind Zeit und Geld. Die vom Bürger gewünschte Relation heißt: so schnell wie möglich, mit möglichst geringem Geldaufwand. Grundsätzlich möchte er nicht unnötig belastet oder in Anspruch genommen werden. Aufwand und Nutzen müssen in angemessenem Verhältnis zueinander stehen.

Was erwartet der Bürger konkret? Er möchte so schnell und einfach wie möglich die für die geplante Aktion zuständige Stelle identifizieren. Wenn möglich, möchte er nur einen Ansprechpartner in der Behörde erhalten. Er möchte umfassend informiert werden und, falls notwendig, darüber beraten werden, was er für die geplante Aktion tun muss. Er möchte Informationen erhalten, die für die Abbildung seiner individuellen Situation verwertbar sind, dazu gehören Informationen über alle notwendigen Unterlagen. Er möchte die ihm gelieferten Informationen verstehen und nachvollziehen können.

Erwartungen des Bürgers

Er möchte über Risiken und Chancen bei der Ausführung der Aktion aufgeklärt werden. Grundsätzlich möchte er bei der Erledigung der Aktion nicht auf die Hilfe Dritter angewiesen sein. Grundsätzlich möchte er für die Aktion keine Hilfsmittel benutzen, die einem üblichen Haushalt nicht zur Verfügung stehen (Kopierer, Faxgerät), weil ihm dadurch zusätzliche Wege und Kosten zugemutet werden. Grundsätzlich möchte er die Behörde nur wenn nötig physisch aufsuchen, um die geplante Aktion durchführen zu können, weil dadurch ebenfalls Kosten und Wegezeiten anfallen. Soweit die Aktion einer Vorbereitung bedarf, ist es erwünscht, dass die Vorbereitung außerhalb der Arbeitszeit des Bürgers erfolgen kann. Er möchte für die Durchführung nicht mit unangemessenen Gebühren oder Nebenkosten (Telefon, Porto, Briefumschläge) belastet werden.

Er möchte, dass sich Rückfragen für die Bearbeitung seiner Aktion im unbedingt erforderlichen Rahmen halten. Er erwartet, dass seine Aktion möglichst schnell bearbeitet wird. Er erwartet freundlich, kompetent und höflich behandelt zu wer-

den. Er möchte der Behörde gegenüber als gleichberechtigter Partner auftreten können und erwartet, dass seine Angelegenheiten vertrauensvoll behandelt werden.

1.2.1 Typischer konventioneller Ablauf eines Bürger-Behörde-Kontakts (Antragsverfahren)

1. Der Bürger ermittelt, welche Behörde für seine beabsichtigte Aktion zuständig ist. Er nutzt dazu das Telefonbuch oder die Telefonauskunft. Er erhält eine Telefonnummer.
2. Er ruft die Behörde mit der ermittelten Telefonnummer an und lässt sich von der Zentrale mit einem zuständigen Bearbeiter verbinden.
3. Er bittet den zuständigen Bearbeiter bei der Behörde, ihm Informationen und Anträge/Formulare per Post zuzusenden.
4. Er füllt den Antrag aus, unterschreibt ihn, fügt die erforderlichen Anlagen bei und sendet ihn an die Behörde zurück. Falls eine darüber hinausgehende Authentisierung notwendig ist, muss er bei der Behörde persönlich erscheinen.
5. Der Antrag wird in der Behörde bearbeitet, ggf. werden noch fehlende Informationen oder Anlagen nachgefordert.
6. Der Bürger erhält den Bescheid von der Behörde per Post. Falls Gebühren oder Kosten fällig werden, werden diese vom Konto des Bürgers abgebucht.

1.2.2 Voraussetzungen für die Nutzung von Online-Angeboten

Der Bürger benötigt in der Regel

- einen üblichen PC und ein Gerät zur Bildschirmausgabe (Monitor),
- einen Telefonanschluss und ein Telekommunikationsgerät, mit dem er Kontakt zum Internet herstellen kann,
- entsprechende Software (zumindest einen Browser), die es ermöglicht Web-Inhalte auszugeben,
- ein Vertragsverhältnis (dauerhaft oder Call-by-Call) mit einem Internet-Service-Provider, der ihm den Zugang zum Internet eröffnet,
- ein E-Mail-Konto, um über das Internet an ihn adressierte Nachrichten empfangen zu können.

Soweit die Dienstleistung nicht vollständig online angeboten wird, ist darüber hinaus ein Drucker und Verbrauchsmaterial erforderlich, um Anträge und Dokumente ausdrucken zu können.

Wird die Dienstleistung vollständig online angeboten, wird in der Regel zusätzliche Hard- und Software benötigt, um sich der Behörde gegenüber ausreichend authentisieren und um rechtsverbindlich elektronisch signieren zu können.

Hard- und Software

Der Bürger benötigt bestimmte Basis-Kenntnisse, um mit der technischen Ausstattung und der Software die erwünschten Ergebnisse erzielen zu können. Er muss in der Lage sein, bestimmten Online-Vorgehensweisen folgen zu können.

Technische Basis-Kenntnisse

Es gibt Personen bzw. bestimmte Bevölkerungsgruppen, für die die Realisierung der vorgenannten Mindestvoraussetzungen aus persönlichen oder finanziellen Gründen nur schwer erfüllbar ist. Deshalb wird es auf absehbare Zeit nicht möglich sein, Dienstleistungen ausschließlich online anzubieten.

1.2.3 Motivation des Bürgers für die Nutzung von Online-Dienstleistungen

In der Regel wird der Bürger den beschriebenen Aufwand nur betreiben, wenn ihm das Online-Angebot entsprechend große Vorteile gegenüber der konventionellen Verfahrensweise bringt. Die Kontaktaufnahme kann aus unterschiedlichen Motiven oder Anlässen heraus erfolgen:

- Allgemeiner Informationsbedarf (z. B. Informationen über eine Behörde)
- Anlassbezogener Informationsbedarf (z. B. aufgrund einer Fernsehsendung o. Ä.)
- Gezielte Recherche (z. B. Suche nach einer zuständigen Behörde, Suche nach Statistiken, Suche nach Pressemeldungen)
- Anforderung von Informationsmaterial (z. B. Broschüren)
- Konkretes Vorhaben (z. B. Absicht, einen bestimmten Antrag zu stellen)
- Beschwerde, Lob

1.2.4 Typischer Ablauf (online) eines Bürger-Behörde-Kontakts (Antragsverfahren)

Der Ablauf bei der Erledigung eines konkreten Vorhabens soll näher betrachtet werden. Er schließt die meisten Schritte bei den anderen Anliegen mit ein.

1. Der Bürger sucht die zuständige Behörde in einem Portal oder mit einer Suchmaschine.
2. Der Bürger nutzt den gefundenen Link zur Weiterleitung zum Web-Auftritt der zuständigen Behörde.
3. Der Bürger sucht über eine Suchfunktion die von ihm gewünschte Online-Dienstleistung und wählt diese an.
4. In der Präsentation der Online-Dienstleistung wählt er die zu ihm passende Option.
5. Er baut eine sichere Verbindung zum Web-Server der Behörde mit dem gewünschten Inhalt auf.
6. Er informiert sich über die Inhalte, Anspruchsvoraussetzungen und das weitere Verfahren für die gewünschte Online-Dienstleistung.

7. Er lädt sich den gewünschten Antrag auf sein lokales PC-System herunter.
8. Er füllt den Antrag mit einer lokalen Anwendung aus.
9. Er versendet den Antrag mit den erforderlichen Anlagen in Dateiform, ggf. als elektronisch signierte E-Mail an die Behörde.
10. Die Behörde prüft den eingereichten Antrag des Bürgers. Der Bürger erhält die Bewilligung seines Antrags als digital signiertes Dokument per E-Mail.
11. Kosten oder Gebühren werden vom Konto des Bürgers abgebucht.

Bei den Schritten 6 und 8 können Fragen auftreten, die der Bürger gerne per E-Mail mit der Behörde klären möchte.

1.3 Qualitätskriterien

Die Kriterien für ein bürgerfreundliches und sicheres Online-Angebot kann man nach den Phasen des Ablaufs eines Online-Kontakts mit einer Behörde, nach den durch den Bürger in Anspruch genommenen Funktionen eines Online-Kontakts und nach einzelnen Anforderungsarten bzw. Anforderungsprofilen des Bürgers gliedern. In diesem Modul wird eine Kombination aus diesen Gliederungskriterien gewählt.

1.3.1 Zugang

Zunächst sollte geprüft werden, wie leicht und gut zugänglich das Angebot für die Kunden ist. Dies beginnt entsprechend dem oben geschilderten Szenario und Ablauf beim Auffinden in einem Portal oder einer Suchmaschine. Ein gefundenes Angebot sollte dann mit den üblichen technischen Mitteln aufgerufen, dargestellt und benutzt werden können – und dies mit vertretbaren Antwortzeiten. Dabei muss entsprechend den Bestimmungen für die barrierefreie Gestaltung auch an die Zugänglichkeit für Menschen mit Behinderungen gedacht werden.

Über die technische Bedienbarkeit hinaus ist dann die inhaltliche Erschließung dafür entscheidend, ob der Benutzer in einem umfangreicheren Angebot schnell und problemlos zu der von ihm gewünschten Information oder Dienstleistung gelangt.

Im weiteren Sinne gehört zu diesem Bereich auch die software-ergonomische Gestaltung im Sinne der Anpassung der Darstellungen, der Dialoggestaltung und Navigation an die menschlichen Fähigkeiten und Bedürfnisse. Die Anforderungen an die software-ergonomische Gestaltung von Web-Seiten werden in so genannten Styleguides zusammengestellt und häufig durch vorgegebene Musterseiten (Templates) praktisch umgesetzt. Für die Bundesbehörden gibt es den IVBB-Intranet-Styleguide.

1.3.2 Qualität von Inhalt und Funktionen

Informationsangebote sollten so gestaltet sein, dass der Bürger möglichst auf alle Fragen zu der Behörde und ihren Dienstleistungen schnell und einfach eine be-

riedigende Antwort erhält. Dies gelingt zwar nie ganz vollkommen, weil die insgesamt gestellten Fragen so vielfältig sind und nur begrenzte Mittel zu Verfügung stehen. Es muss auch nicht jede Frage abschließend beantwortet werden. Vielfach ist der Bürger auch zufrieden, wenn er erfährt, an wen er sich mit seiner konkreten Frage wenden kann.

Informationsangebote sollten hinreichend breit und tief sein. Die Breite bezieht sich auf die Vollständigkeit hinsichtlich des gesamten Themenkatalogs, der sich aus dem Zweck und dem Dienstleistungsangebot ergibt. Die Tiefe betrifft die Ausdifferenzierung und Detaillierung der einzelnen Themengebiete vom zusammenfassenden Überblick bis zur Detailinformation.

Informations-
angebote

Aus der Sicht des Bürgers kommt es letztlich darauf an, dass typische Informationsbedürfnisse gut erfüllt werden. Diese betreffen insbesondere

- Orientierungsinformationen über die Behörde, wie Aufgaben, Organisation, Dienstleistungsspektrum,
- Aufgaben und Leistungen, u. a. was kann man wo und wie erledigen (Erreichbarkeit der Ansprechpartner, Unterlagen).

Besonders hervorzuheben ist die Möglichkeit, Informationsmaterial online anzufordern. Als Qualitätskriterien für dieses gesamte Informationsangebot werden die Verständlichkeit, Korrektheit und Vertrauenswürdigkeit sowie die Aktualität herausgestellt.

Das Kommunikationsangebot umfasst in der Regel E-Mail, Newsletter und Mailing-Listen sowie Diskussionsforen und Chats. In Bezug auf E-Mails kommt es vor allem auf die Erreichbarkeit der Stellen mit Kundenkontakt an.

Kommunikations-
angebote

Bei den übrigen Kommunikationsangeboten kommt es sowohl auf den gezielten und dosierten Einsatz als auch auf die sach- und zielgruppengerechte Ausgestaltung an. Ein Forum, bei dem es kaum Diskussionsbeiträge gibt, ist ebenso wenig ein Zeichen guter Kommunikationspolitik wie eine Mailingliste, über die jeden Tag 30 Mails mit überwiegend an einzelne Personen gerichtete Mitteilungen an einen großen Empfängerkreis verschickt werden.

Transaktionsangebote beinhalten die rechtsverbindliche Einleitung und ggf. Abwicklung von Verwaltungsangelegenheiten. Auch hier sind Breite und Tiefe des Angebots ein wichtiger Maßstab. Die Breite betrifft den Umfang der online angebotenen Dienstleistungen bzw. Geschäftsprozesse, die Tiefe bezieht sich auf die Komplexität, in der ein Geschäftsprozess über alle Schritte hinweg online abgebildet und komplett abgeschlossen werden kann.

Transaktions-
angebote

Die Qualität eines solchen Angebots wird insbesondere durch die Einbindung in das Gesamtangebot, den Aufwand, die Medienbruchfreiheit, die Plattformunabhängigkeit und die Art der Handhabung bestimmt. Dazu gehören auch die angebotenen Hilfsfunktionen und die Bezahlmöglichkeiten (Payment).

1.3.3 IT-Sicherheit

Da viele potenzielle Nutzer aufgrund von Sicherheitsbedenken Transaktionsangebote nicht in Anspruch nehmen, ist eine Überprüfung und Verbesserung der

Sicherheit des Web-Angebots von ganz besonderer Bedeutung. Dabei werden fünf Teilbereiche betrachtet:

- IT-Sicherheitsmanagement,
- aktive Inhalte,
- Kryptografie, Verbindungssicherheit und Authentisierung,
- Absicherung von Web-Servern per Firewall sowie
- die Administration von Web-Servern.

Die einzelnen Problemstellungen und Handlungsmöglichkeiten zu diesen Punkten werden in anderen Modulen des E-Government-Handbuchs ausführlich dargestellt. In diesem Modul geht es daher lediglich um eine zusammenfassende Überprüfung und um Hinweise auf mögliche Maßnahmen, die an anderer Stelle näher beschrieben werden.

1.3.4 Datenschutz

IT-Sicherheit bezieht sich primär auf den Schutz des IT-Systems (Hardware, Software, Daten) vor Verlust sowie unbefugter Nutzung oder Veränderung. In engem Zusammenhang mit diesen Aspekten geht es beim Datenschutz speziell um den Schutz der Nutzer vor unzulässigen Eingriffen in ihre Privatsphäre.

Was zulässig ist und was nicht, und welche Vorkehrungen zu treffen sind, ist in den allgemeinen und in bereichsspezifischen Gesetzen und Verordnungen geregelt. Hier sind insbesondere das Bundesdatenschutzgesetz und das Teledienstedatenschutzgesetz (TDDSG) zu nennen. Die Hauptanforderungen sind gleichzeitig die wichtigsten Qualitätskriterien. Sie betreffen

- die Transparenz in Bezug auf die speichernde Stelle sowie ihre Datenschutz- und Sicherheitspolitik,
- die materielle Rechtmäßigkeit der Datenverarbeitung, insbesondere aufgrund freiwilliger Einwilligungen in Bezug auf Speicherung, Verarbeitung, Übermittlung und Auswertung von personenbezogenen Daten,
- den Bereich der Datensparsamkeit.

1.3.5 Verantwortlichkeit für Inhalte

Nicht nur, um den Qualitätsansprüchen der Nutzer gerecht zu werden, sondern auch, um die haftungsrechtlichen Risiken den jeweiligen Verantwortlichen richtig zuzuordnen, wird abschließend auf die Verantwortlichkeit für Inhalte und den Jugendschutz näher eingegangen. Vor dem Hintergrund jüngster Gerichtsentscheidungen der Land- und Oberlandesgerichte ist es für die Behörde wie für jeden anderen Internetdienstleister wichtig, die Verantwortlichkeit für die von ihr präsentierten Inhalte klar und verständlich von anderen abzugrenzen. Es werden daher neben einer zusammenfassenden Darstellung der für die Verantwortlichkeit relevanten §§ 9 – 11 des Teledienstegesetzes auch Abgrenzungskriterien für die Unterscheidung zwischen eigenen und fremden Inhalten genannt. Hinweise zur

regelmäßigen Kontrolle der Inhalte sowie Erläuterungen zum Jugendschutz schließen dieses letzte Kapitel ab.

1.4 Prioritäten, Hilfe zur Bewertung

Der Leser, der mit den inhaltlichen Empfehlungen der Qualitätskriterien arbeiten möchte, sollte sich frühzeitig Gedanken machen, wie er festgestellte Abweichungen vom Soll-Ist-Zustand bewertet und in welcher Reihenfolge er diese Differenzen beseitigen möchte. Die folgende Skalierung kann dabei als Grundlage dienlich sein.

Die Qualitätskriterien werden inhaltlich mit einem Ranking in zwei Dimensionen bewertet, nämlich nach dem Aufwand zur Realisierung des Qualitätskriteriums und nach dessen Bedeutung:

AUFWAND (A)	Definition	Erläuterung zur Definition
1	Sehr gering	Aufwand für eine Person bis zu einem Tag
2	Gering	Aufwand für eine Person mehrere Tage
3	Mittel	Aufwand für eine oder mehrere Personen im Bereich weniger Wochen
4	Hoch	Aufwand sollte projiziert werden. Mehrere Monate.

BEDEUTUNG (B)	Definition	Erläuterung zur Definition
1	Weniger wichtig	Die Nichtbeachtung des Qualitätskriteriums hat keine oder geringe Konsequenzen.
2	Üblich	Der Bürger erwartet, dass dieses Qualitätskriterium erfüllt wird.
3	Wichtig	Die Vernachlässigung des Qualitätskriteriums kann ernsthafte Konsequenzen nach sich ziehen.
4	Elementar	Die Nichterfüllung des Qualitätskriteriums ist für die Behörde imageschädigend.

Das jeweilige Ranking wird in der Randziffer zu Beginn jedes Qualitätskriteriums angezeigt.

Das Ranking kann und soll als Anhaltspunkt für die Überprüfung und Beseitigung von Mängeln in den Web-Inhalten genutzt werden. Es besteht keine direkte Relation zwischen Aufwand und Bedeutung. Gleichwohl wird empfohlen, Mängel mit geringem Aufwand und hoher Bedeutung zuerst zu beseitigen.

Es ist schwierig ein einheitliches Ranking für die Qualitätskriterien aufzubauen, da sich das Ranking von Anwendungsfall zu Anwendungsfall anders darstellt. Die Web-Inhalte einer großen Behörde, die schon seit Jahren Informationen anbietet und dementsprechend schon lange Erfahrungen und Feedback gesammelt hat, sind anders zu bewerten als die einer kleinen Behörde, die gerade erst Anwendungsmöglichkeiten für sich entdeckt.

Häufig ist es schnell geschehen einen Mangel festzustellen, aber aufwändig diesen abzustellen und zu verhindern, dass der erreichte positive Stand auch gesichert bleibt. Es wurde versucht, diese Problematik in die Bewertung des Aufwandes einfließen zu lassen.

Soweit gesetzliche Vorgaben die Sicherstellung eines Qualitätskriteriums erfordern, wurde die Bedeutung mindestens mit 3 (Wichtig) angesetzt.

1.5 Checkliste

Am Ende des Moduls findet sich eine Checkliste, in der zu den Qualitätskriterien konkrete Prüffragen formuliert sind. Diese sollten mit Ja oder Nein beantwortet werden. Ein Nein verweist dann darauf, dass noch Verbesserungen möglich sind, für die in den entsprechenden Abschnitten 2 – 6 dieses Moduls Empfehlungen gegeben werden.

Die Bezeichnung „Empfehlungen“ soll ausdrücken, dass die jeweils genannten Maßnahmen aufgrund der Erfahrung der Autoren geeignet sind, die Qualitätsanforderungen zu erfüllen. Hierbei handelt es sich jedoch weder um die einzig mögliche Maßnahme, noch ist der Erfolg der Maßnahme garantiert. Kaum eine der empfohlenen Maßnahmen kann isoliert die Qualität steigern. Hintergrund- und Kontextwissen ist erforderlich, um die Empfehlungen in ein angemessenes Handlungskonzept umzusetzen.

Empfehlungen

2 Zugang

Das beste Online-Serviceangebot nutzt wenig, wenn es den Bürgerinnen und Bürgern nicht bekannt ist, es nicht zugänglich ist oder nicht genutzt werden kann. Wer in den Weiten des Internets gefunden werden will, muss sein Angebot über Suchmaschinen und Verzeichnisse bekannt machen. Aus technischer Sicht sind weiterhin die Kompatibilität mit der von den Nutzerinnen und Nutzern eingesetzten Technik sowie die Performanz des Angebots von entscheidender Bedeutung. Zur inhaltlichen Erschließung gehört es, die Orientierung im Angebot so einfach wie möglich zu machen, eine interne Suchfunktion anzubieten, relevante Teile mehrsprachig und barrierefrei zu gestalten, eine zielorientierte Navigation zu ermöglichen und Hilfen für gegebenenfalls auftretende Probleme anzubieten.

2.1 (Technische) Zugänglichkeit und Auffindbarkeit

2.1.1 Auffindbarkeit im Internet

Angesichts der über das Internet zugänglichen Informationsfülle ist es für jeden Anbieter eines Web-Angebots unverzichtbar, sein Angebot unter einer möglichst einprägsamen und nachvollziehbaren Web-Adresse (URL: Uniform Resource Locator) direkt auffindbar zu machen.

Einprägsame und verständliche URLs

Bei der Wahl der URL sollten daher die bei Web-Angeboten im Allgemeinen und Verwaltungsseiten im Besonderen üblichen Konventionen eingehalten werden. Stadtverwaltungen lassen sich in der Regel über www.stadtnamen.de, die Bundesländer über www.bundesland.de finden. Für nachgeordnete Landes- oder Bundesbehörden existieren bei der Wahl einer URL mehrere Alternativen, die in Anbetracht der niedrigen Kosten, die mit der Belegung einer Web-Adresse verbunden sind, möglichst alle angeboten werden sollten.

**Abschnitt 2.1.1:
Aufwand 2,
Bedeutung 4**

Gängige Adressmuster auf Bundesebene sind u. a.: www.behoerdenname.de (z. B. www.auswaertiges-amt.de oder www.bundesfinanzministerium.de), www.behoerdenkuerzel.de (z. B. www.bzga.de der Bundeszentrale für gesundheitliche Aufklärung) oder www.behoerdenkuerzel.bund.de (z. B. www.bmi.bund.de des Bundesinnenministeriums). Da die Abkürzungen von Behörden den Bürgerinnen und Bürgern nicht unbedingt bekannt sind, sollten diese nur ergänzend Verwendung finden. So ist beispielsweise das Bundesministerium für Familie, Senioren, Frauen und Jugend über die URL www.bmfsfj.de, aber auch über www.bundesfrauenministerium.de zu finden. Auch die Eingaben „bundesjugendministerium“, „bundesfamilienministerium“ oder „bundesseniorenministerium“ führen zum Erfolg.

In den Bundesländern sind www.behoerdenname.bundesland.de, www.behoerde-bundesland.de oder www.bundesland.de/behoerdenname geläufige Schemata. Auch hier werden häufig die Behördenkürzel alternativ oder ergänzend zum vollen Behördennamen verwendet.

Bund, Länder und Kommunen können zusätzlich auch solche Web-Adressen belegen, die häufigen Schreibfehlern oder Buchstabendrehern Rechnung tragen.

Zumindest bei komplizierten Behörden- oder Ortsnamen sollte dies bedacht werden.

Zusätzlich zur Wahl einer einprägsamen URL empfiehlt es sich, das Angebot bei möglichst vielen Suchmaschinen und Verzeichnissen anzumelden. Auf diese Weise können die Seiten auch dann gefunden werden, wenn ein Bürger gar nicht nach einer einzelnen Behörde, sondern nach Informationen zu bestimmten Themen sucht.

Verzeichnisse und Suchmaschinen

Für die Recherche im Internet stehen zum einen Verzeichnisse oder Kataloge und zum anderen Suchmaschinen zur Verfügung:

- Verzeichnisse (wie z. B. Yahoo oder Web.de) verwenden zur Indizierung einer Webseite in der Regel die Angaben, die deren Anbieter in ein Anmeldeformular eingetragen hat. Vor der Übernahme ins Webverzeichnis werden diese Eingaben redaktionell geprüft. Da im Verzeichnisindex später nur wenige Angaben aufgeführt werden, ist es wichtig, Titel, Beschreibung und Suchbegriffe sorgfältig zu wählen, damit die Seiten von der Redaktion aufgenommen, korrekt in die Systematik des Verzeichnisses eingeordnet und zutreffend beschrieben werden können.
- Suchmaschinen (wie z. B. Google, Lycos, InfoSeek, Fireball oder AltaVista) starten nach der Anmeldung einer Seite durch deren Anbieter Suchprogramme (z. B. Robots, Spider, Crawler), die die Webseite(n) nach speziellen Merkmalen durchforsten. Von besonderer Bedeutung sind Metadaten („Daten über Daten“), die als Bestandteil einer Webseite Auskunft über deren Art und Inhalt geben. Metadaten werden als solche gekennzeichnet und im Kopf (Header) eines HTML-Dokuments platziert, sodass sie in der Normalansicht vom Browser nicht dargestellt werden. Sie sollten insbesondere Angaben zu den Autoren und zum Inhalt, charakteristische Stichwörter und das Publikationsdatum enthalten. Alle von den Robots recherchierten Merkmale werden an die Suchmaschine zurückgemeldet und dienen der gezielten Indizierung der Seite(n). Suchmaschinen nehmen wesentlich mehr Daten in ihren Index auf als Webverzeichnisse. Dies können neben Titel und Metadaten auch die ersten Zeilen einer Webseite oder sogar das ganze Web-Dokument (Volltext-Index) sein.

Zum Teil ist die Aufnahme in ein Webverzeichnis oder den Index einer Suchmaschine kostenpflichtig. Dabei werden meist unterschiedliche Tarifmodelle angeboten, die den speziellen Bedürfnissen der Seitenanbieter Rechnung tragen sollen. Um unnötige Kosten zu vermeiden und eine gute Auffindbarkeit des eigenen Angebots zu gewährleisten, sollte sich ein Anbieter zumindest in der Anfangsphase auf die aus seiner Sicht wichtigsten Verzeichnisse und Suchmaschinen konzentrieren. Inzwischen gibt es auch eine Reihe von meist kostenpflichtigen Online-Services bzw. Software-Angeboten, mit denen sich die Anmeldung bei Verzeichnissen und Suchmaschinen (teil)automatisieren lässt. Bei der Auswahl eines solchen Dienstes oder Programms sollte darauf geachtet werden, welche Verzeichnisse und Suchmaschinen mit den benötigten Angaben beliefert werden.

Ergänzend zu den „web-üblichen“ Verzeichnisdiensten und Suchmaschinen sollten Anbieter von Verwaltungsseiten darauf achten, dass ihre Seiten auch über einschlägige Behördenportale (z. B. www.bund.de oder die Startseite eines Bundeslandes) erreichbar sind. Sofern keine Online-Registrierung vorgesehen ist, wird

Behördenportale

sich dies im Kontakt mit dem zuständigen Webmaster arrangieren lassen. Darüber hinaus ist es aus Bürgersicht stets hilfreich, wenn inhaltlich benachbarte Web-Angebote anderer Behörden durch einen Link angebunden werden. Daher sollte darauf geachtet werden, dass die eigenen Seiten in den Linklisten thematisch verwandter Angebote aufgeführt sind. Grenzen zwischen Ressorts oder Gebietskörperschaften sollten dabei kein Hindernis darstellen, schließlich ist aus Bürgersicht allein die inhaltliche Nähe maßgeblich.

Ein weiterer Zugang zu Internetangeboten führt über die Liste der Favoriten („Bookmarks“), die der Bürger in seinem Browser hinterlegen kann. Im nicht dargestellten Kopf einer Webseite („Header“) können Zusatzinformationen eingetragen werden, die dann in der Bookmark-Liste des Bürgers erscheinen und diesem das Wiederfinden der gewünschten Seite erleichtern. Da dieser Text sehr kurz gehalten werden muss, empfiehlt sich bei Verwaltungsseiten in der Regel der Eintrag des Behördennamens.

Bookmarks

2.1.2 Kompatibilität

2.1.2.1 Browserversionen

Bei der Darstellung von Webseiten treten in Abhängigkeit vom Browser, den der Betrachter gerade nutzt, häufig deutliche Unterschiede auf. Aus diesem Grund sollte regelmäßig kontrolliert werden, wie die geläufigsten Browser (z.B. Internet Explorer, Netscape/Mozilla, Opera) das eigene Angebot darstellen. Generell sollten Webseiten mit möglichst vielen Browsern ohne Einschränkungen genutzt werden können. Orientiert sich eine Seitengestaltung dennoch stark oder sogar ausschließlich an den Anforderungen eines bestimmten Browsers, führt dies häufig zu Problemen beim Seitenaufruf mit einem anderen Produkt. In diesen Fällen sollte dem Bürger deutlich mitgeteilt werden, für welchen Browser die Optimierung vorgenommen wurde. Nicht selten stehen auf einem PC mehrere Browser zur Verfügung, sodass der Bürger durch den einfachen Wechsel des genutzten Programms die Darstellung auf seinem Gerät deutlich verbessern kann.

**Abschnitt 2.1.2.1
Aufwand 2, Bedeutung 2**

Darstellungsprobleme können sich auch aus der Verwendung älterer Programmversionen oder bei der Nutzung weniger gebräuchlicher Browser, etwa dem rein textbasierten Lynx-Browser, ergeben.

2.1.2.2 Alt-Texte

Die Kompatibilitätsprobleme sind grundsätzlich um so größer, je mehr zusätzliche Elemente wie Frames, Bilder etc. verwendet werden. Daher sollte ergänzend eine „Nur-Text-Version“ angeboten werden, bei der Grafiken durch so genannte ALT-Tags (Alternativtext, s. Abb. 3) erweitert werden.

„Nur-Text-Version“

Auf diese Weise erfährt der Bürger auch ohne aktivierte Grafikanzeige oder mit einem textbasierten Browser vom Inhalt einer Abbildung, die er sich bei Interesse dann doch anzeigen lassen kann. Dazu kann er z. B. seine Browsereinstellung entsprechend ändern, einen „herkömmlichen“ Browser oder ein Bildbetrachtungs-

**Abschnitt 2.1.2.2
Aufwand 1, Bedeutung 4**

bzw. -bearbeitungsprogramm verwenden. Für Bürger, die gebräuchliche Technik nach aktuellem Stand der Entwicklung einsetzen, können selbstverständlich dennoch Animationen, Grafiken usw. angeboten werden. Nur sollten solche „Extras“ eben nicht zu Einschränkungen für andere Nutzergruppen führen. Eine solche Herangehensweise kann auch die Performanz über schmalbandige Zugänge (s. 2.1.3) verbessern und kommt zugleich der Anforderung entgegen, Web-Angebote der Verwaltung barrierefrei zu gestalten (s. 2.2.4).



Abb. 1: Ansicht einer Grafik im Internet Explorer 5.5 („Bilder anzeigen“ eingeschaltet, Standardeinstellung)

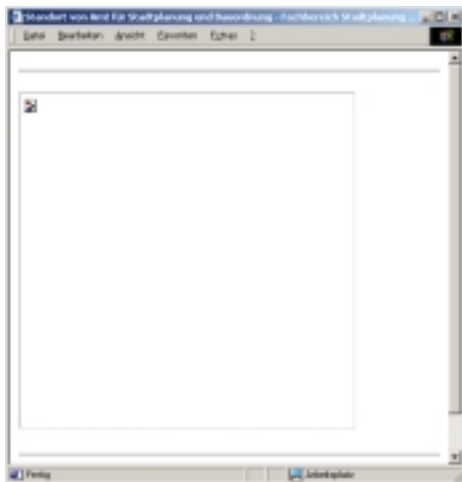


Abb. 2: Ansicht einer Grafik im Internet Explorer 5.5 („Bilder anzeigen“ manuell ausgeschaltet) ohne alternativen Text

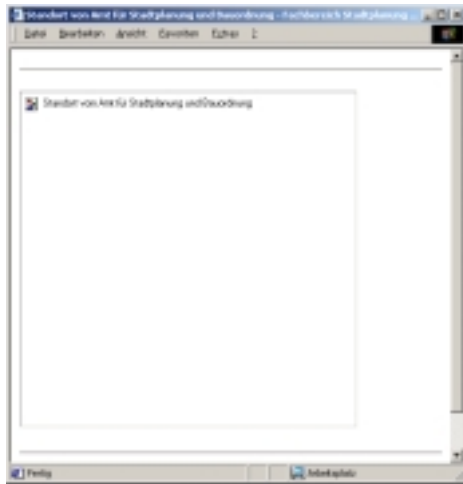


Abb. 3: Ansicht einer Grafik unter Internet Explorer 5.5 („Bilder anzeigen“ manuell ausgeschaltet) mit alternativem Text¹

2.1.2.3 Plug-Ins

Um auch Datenformate, die den Browsern unbekannt sind, direkt in eine Webseite integrieren zu können, werden Plug-Ins verwendet. Bekannte Plug-Ins sind z. B.:

- Acrobat Reader (zum Betrachten von PDF-Dateien)
- Apple Quicktime (Video-/Audio-Player)
- Flash (zur multimedialen Gestaltung von Internetseiten durch Sound und Animationen)
- Realplayer (Video-/Audio-Player)
- Windows MediaPlayer (Video-/Audio-Player)

**Abschnitt 2.1.2.3
Aufwand 1, Bedeutung 3**

Für den Bereich der Bundesverwaltung hat die Projektgruppe BundOnline 2005 im Rahmen des Projekts „Standards und Architekturen für E-Government-Anwendungen“ (SAGA) auch für die Verwendung von Plug-Ins Empfehlungen ausgesprochen.²

SAGA-Empfehlungen zu Plug-Ins

In den neueren Browserversionen sind zahlreiche solcher Plug-Ins bereits vollständig installiert und werden standardmäßig ausgeführt. Nutzer älterer oder „exotischer“ Programmtypen hingegen müssen die zusätzlich benötigte Software unter Umständen erst noch laden und installieren, was den Aufwand bei der Angebotsnutzung deutlich erhöht. Da auch nicht davon ausgegangen werden kann, dass die Bürger mit Plug-Ins ebenso vertraut sind wie mit den Funktionalitäten

¹ Mit einer Beschreibung in HTML () erscheint der Alternativtext bei einem „Mouse over“ (Führen der Maus über das Bild bzw. den Bildrahmen) oder beim Abschalten der Grafikanzeige. (Die Darstellung in den Abbildungen entspricht nicht den Originalseiten unter www.bremen.de, sondern wurde zur Verdeutlichung der Funktionsweise von Alternativtexten angefertigt.)

² <http://www.bund.de/saga>. Die hier veröffentlichten Vorgaben und Empfehlungen werden umgehend nach Freigabe im E-Government-Handbuch veröffentlicht.

ihres Browsers, sollte genau geprüft werden, ob solche Extras tatsächlich erforderlich sind. Ohne Zweifel können Plug-Ins den Gebrauchswert eines Web-Angebots deutlich erhöhen. Um aber Personen, die Plug-Ins nicht nutzen können oder wollen, nicht auszuschließen, sollte stets kritisch geprüft werden, ob eine Verwendung dieser Zusatzprogramme tatsächlich unverzichtbar ist. Kommt ein Plug-In vor allem aus optischen Gründen zum Einsatz, sollte auch eine alternative Seitendarstellung angeboten werden, die Ladezeiten spart und keine zusätzlichen Installationen erfordert.

2.1.2.4 Bildschirmauflösung

Eine Zeit lang wurde empfohlen, die Darstellung einer Webseite auf eine bestimmte Bildschirmgröße (z. B. 800 x 600 oder 1024 x 768 Pixel) hin zu optimieren. Angesichts der heute anzutreffenden Systemvielfalt (alte vs. neue Grafikkarten und Monitore, diverse Monitorgrößen für stationäre PCs und Notebooks, kleine Monitore an Mobilgeräten usw.) erscheint dies nicht mehr empfehlenswert. Die Überlegung, eine optimierte Darstellung anzubieten, setzt zudem voraus, dass die Bürger ihren Browser im Vollbildmodus nutzen. Auch dies ist, gerade wenn jemand mehrere Fenster geöffnet hat, häufig nicht der Fall.

Abschnitt 2.1.2.4
Aufwand 1, Be-
deutung 3

Aus diesen Gründen sollten sich die Seitengestalter nicht an Bildschirmgrößen orientieren sondern stattdessen prozentuale Breiten- und Höhenangaben verwenden. Wird zur Seiteneinteilung eine Tabelle verwendet, würde beispielsweise die Formatangabe „80 %“ bedeuten, dass die Tabelle 80 % des Browserfensters einnimmt. Der in ihr befindliche Text passt sich dann der vom Bürger gewählten Größe des Browserfensters an. Bei kleineren Fenstern bricht der Text automatisch um, sodass horizontales Scrollen vermieden werden kann.

Prozentuale Brei-
ten- und Höhen-
angaben

Weiterhin sollte die Darstellung so gewählt werden, dass die Standard- oder Default-Einstellungen des jeweiligen Browsers nutzerseitig nicht geändert werden müssen, wohl aber geändert werden können, um z. B. das Schriftbild zu vergrößern. Die ganz überwiegende Mehrheit der Bürger lässt die Voreinstellungen der jeweiligen Browser unverändert, sodass sich die Seitengestaltung an den Default-Werten der aktuell geläufigsten Browser orientieren sollte.

2.1.2.5 Schriftarten

Als weitere Schwierigkeit kommt hinzu, dass es selbst bei Verwendung eines identischen Browsers auf unterschiedlichen Systemen zu technischen und betriebs-systembedingten Abweichungen der Darstellung kommen kann³:

Abschnitt 2.1.2.5
Aufwand 1, Be-
deutung 1

- Manche Betriebssysteme (Unix, Linux und Mac) benutzen eine Bildschirmauflösung von 72 dpi, Windows auf einem PC zeigt dabei 96 dpi an.
- Schriften bzw. Formatierungen werden durch Browser sehr unterschiedlich dargestellt, selbst bei „gleichen“ Versionen eines Browsers können Unterschiede auf verschiedenen technischen Plattformen auftreten.

³ <http://www.webwriting.de/sogehts/cssabweichung.shtml>

- Je nach System können Schriften auch sehr unterschiedlich ausfallen, wenn z. B. unter Unix die „Windows-Verdana“ durch eine „Helvetica“ ersetzt wird.

Derartige Variationen und Probleme lassen sich nie vollständig vermeiden. Gleichwohl sollten Größe und Type einer Schrift so gewählt werden, dass zumindest in der Mehrzahl der Fälle davon ausgegangen werden kann, dass keine Darstellungsprobleme auftreten. Die Schrifttype „Times“ beispielsweise ist in geringer Größe an einem PC mit großem Bildschirm vielleicht gerade noch lesbar, an einem Mac aber schon nicht mehr zu erkennen. Inzwischen existiert eine Reihe von Handbüchern⁴ und Webseiten⁵, die dabei helfen, solch gestalterische Klippen zu umschiffen.

2.1.3 Performanz

Ein weiteres Hindernis auf dem Weg zum Bürger besteht häufig in einer zu langen Ladezeit. Je länger es dauert, bis sich eine Seite am Bildschirm aufbaut, desto größer ist die Wahrscheinlichkeit, dass ungeduldige Bürger den Vorgang abbrechen, bevor das Angebot überhaupt inhaltlich gewürdigt werden konnte. Aus diesem Umstand resultiert für die Anbieter von Web-Angeboten ein echtes Dilemma: Auf der einen Seite verbessert eine grafische Gestaltung die (optische) Attraktivität des Angebots, auf der anderen Seite sind gerade aufwändige Grafiken hauptverantwortlich für lange Ladezeiten.

Abschnitt 2.1.3
Aufwand 3, Bedeutung 4

Das Spektrum der Maßnahmen, um Ladezeiten zu verkürzen, reicht von Verbesserungen an der Struktur des Gesamtangebots über die grafische Gestaltung bis hin zur Seitenprogrammierung, die sich bewusst darum bemüht, den subjektiven Eindruck einer langen Ladezeit beim Anwender zu mildern. Als Faustregel gilt, dass bereits Ladezeiten über acht Sekunden Dauer als problematisch einzustufen sind. Daraus leitet sich beim derzeitigen Stand der nutzerseitig verbreiteten Technik ab, dass Webseiten möglichst nicht größer als 60 bis 70 KB sein sollten. Bei einem Modemzugang benötigen solche Seiten immer noch 15 bis 20 Sekunden Ladezeit. Eine Startseite sollte möglichst noch kleiner und somit noch schneller vollständig lesbar sein.

Ladezeiten verkürzen

Als wichtigste Maßnahmen, um die Übertragungszeit von Webdokumenten zu verkürzen, sind hier zu nennen⁶:

- **Ladezeiten subjektiv verkürzen:** Wartezeiten werden insbesondere dann als störend und schwer erträglich empfunden, wenn der Bürger zu vollständiger Passivität gezwungen wird. Der subjektive Eindruck kann gemildert werden, wenn auf dem Bildschirm Aktivität erkennbar ist und sich der Bürger schon während des Ladevorgangs einen ersten Eindruck vom Angebot machen kann.

⁴ Vgl. u. a. Martina Manhartsberger/Sabine Musil: Web Usability – Das Prinzip des Vertrauens. Bonn: Galileo Press 2001; Jakob Nielsen: Designing Exceptional Websites. Indianapolis: New Riders, 1998; Jakob Nielsen/Marie Tahir: Homepage Usability. 50 enttarnte Websites. München: Markt und Technik, 2002.

⁵ Hilfreiche Hinweise finden sich u. a. auf folgenden Seiten: <http://selfhtml.teamone.de/>, <http://www.netdesign4u.de/tipps/index.php> und <http://www.aboutwebdesign.de/awd/index.shtml>

⁶ <http://www.wk.fu-berlin.de/Reader/neuergo/index.html>

Dieser Effekt kann unterstützt werden, wenn z. B. Grafikhöhen und -breiten vorgegeben werden, sodass ein Browser die Seite schon vor dem Laden der zugehörigen Grafikdateien im richtigen Format darstellen kann. Dieser Effekt wird noch unterstützt, wenn zu Grafiken Alternativtexte angeboten werden, die den Inhalt eines Bildes oder einer Abbildung bis zu deren vollständigem Erscheinen beschreiben.

- **Identische Grafiken verwenden:** Wo immer es sich anbietet, werden identische Grafiken verwendet, die nur einmal geladen werden müssen (z. B. Logos, Icons, Bullets etc.).
- **Grafiken richtig komprimieren:** Die Wahl der Kompressionsmethode sollte sich am verwendeten Grafiktyp orientieren: Bei Fotos und realistischen Bildern wird in der Regel das JPEG/ JPG-Format („Joint Photographic Expert Group“) zu besseren Kompressionsergebnissen führen, während sich das GIF-Format („Graphics Interchange Format“) mit seinen maximal 256 Farben in erster Linie für Bilder mit geringen Farbtiefen eignet. Für Darstellungen im Internet reicht bei JPEG/ JPG die Wahl einer niedrigen Qualitätsstufe. Bei GIF reduziert sich der Speicherbedarf entscheidend, wenn weniger Farben verwendet werden.
- **Bildvorschau anbieten:** Bei umfangreicheren Grafik- oder Fotogalerien kann die Ladezeit durch eine Vorschau mit stark verkleinerten Bildern („thumbnails“), die der Bürger wahlweise durch Anklicken vergrößern kann, reduziert werden.
- **Umfangreiche und komplexe Seiten vermeiden:** Vielfach lassen sich lange Ladezeiten schon dadurch vermeiden, dass umfangreiche Darstellungen auf mehrere, dann schneller zu ladende Seiten verteilt werden.
- **Alternative Seitenversionen anbieten:** Da das Verwenden von Frames, Grafiken, Plug-Ins usw. die Ladezeiten in der Regel erheblich erhöhen kann, sollte für Bürger mit älterer Technik oder schmalbandigen Anschlüssen eine schneller ladbare Version angeboten werden, die auf aufwändige Grafik und weitere Extras so weit wie möglich verzichtet (s. dazu auch 1.1.2). Dabei sollte auf eine dennoch ansprechende Präsentation geachtet werden, indem z. B. lange Texte vermieden oder durch Zwischenüberschriften, Hervorhebungen u.ä. aufgelockert werden.

Um die technische Zugänglichkeit des eigenen Angebots aus Sicht der Adressaten beurteilen zu können, empfehlen sich Tests, bei denen die Seiten u. a. über eine schmalbandige Anbindung aufgerufen und mit unterschiedlichen Browsern und Betriebssystemen genutzt werden. Nur so lässt sich erkennen, ob die Seiten in akzeptabler Zeit laden bzw. ob Kompatibilitäts- oder Darstellungsprobleme auftreten.

2.2 (Inhaltliche) Erschließung

2.2.1 Allgemeine Orientierung

Nachdem die Bürgerinnen und Bürger das Angebot einer Verwaltung gefunden bzw. aufgerufen haben, sollte ihnen dort die Orientierung so leicht wie möglich gemacht werden. Sie sollten sich schnell einen Überblick über Struktur und Angebot machen können, um die benötigte Information oder eine spezielle Dienstleistung ohne Umwege und Irritationen zu finden.

Überblick über
Struktur und
Angebot schaffen

Einmal im Angebot der Verwaltung „unterwegs“, sollte der Nutzer jederzeit erkennen können, wo er sich gerade befindet (also z. B. in welcher Rubrik er gerade navigiert) und welche weiteren Angebote der von ihm aktuell aufgerufenen Seite vor- oder nachgelagert sind. Dieser allgemeinen Orientierung dienen insbesondere Inhaltsverzeichnis und Sitemaps.

Abschnitt 2.2.1
Aufwand 3, Be-
deutung 3

„Inhaltsverzeichnisse“ eignen sich vor allem zum Überblick über große, hierarchisch aufgebaute Web-Angebote. Ein Inhaltsverzeichnis sollte in der Standard-einstellung zunächst nur die oberen Gliederungsebenen anzeigen, es den Bürgern aber erlauben, auf Wunsch weitere Hierarchieebenen einzublenden. Ergänzend zum Inhaltsverzeichnis stellt eine „Sitemap“ als verweissensitive Grafik die Struktur des Internetangebots in seiner Gesamtheit dar, ähnlich wie ein Organigramm den Aufbau komplexer Behörden oder Unternehmen wiedergibt. Sitemaps erlauben es, sich auf einen Blick über die angebotenen Rubriken und zugehörigen Unterpunkte zu informieren. Sowohl vom Inhaltsverzeichnis als auch von der Sitemap kann das gewünschte Angebot direkt aufgerufen werden. Ein Inhaltsverzeichnis gibt stets die von den Anbietern präferierte Gliederungslogik wieder. Ist diese Struktur gut durchdacht bzw. denkt der Bürger in ähnlichen Kategorien, ist das Inhaltsverzeichnis zur allgemeinen Orientierung gut geeignet. Ersatzweise oder ergänzend ermöglicht die Sitemap eine stärker intuitiv gesteuerte Orientierung.

Inhaltsverzeich-
nisse

Bei der Gestaltung der Struktur eines Internetangebots sollte die Sichtweise der Bürgerinnen und Bürger zu Grunde gelegt werden.⁷ Beispielsweise erscheint es wenig sinnvoll, sich bei der Festlegung von Gliederungsebenen an der Organisationsstruktur einer Verwaltung zu orientieren, da diese den Bürgern in der Regel nicht bekannt ist. Verallgemeinernd lässt sich festhalten, dass eine wenig durchdachte Struktur von gut gestalteten Inhaltsverzeichnissen und Sitemaps nur bedingt kompensiert werden kann.

Als weitere Orientierungshilfen haben sich Einstiegsmöglichkeiten für bestimmte Zielgruppen bewährt. Bürger treten mit anderen Erwartungen und Wünschen an die Verwaltung heran als Unternehmen, diese haben wieder andere Bedürfnisse als etwa Angehörige von Berufsgruppen, die regelmäßig im Auftrag Dritter Kontakt mit bestimmten Verwaltungen haben, oder als Mitarbeiter anderer Verwaltungen. Diesen Unterschieden kann dadurch Rechnung getragen werden, dass

Zielgruppen-
orientierung

⁷ Vgl. dazu auch die Ausführungen im Modul „Phase 2 – Strategie“ (insbes. Aktivität 2.1) sowie im Modul „Bewertungskriterien für potenziell online-fähige Dienstleistungen“ (IV A), Kapitel 2.

schon auf der Startseite eines Angebots nach der „Rolle“ eines Bürgers gefragt wird. Je nach Auswahl wird ihm dann eine entsprechend aufbereitete Seite angeboten, die direkt auf jene Angebotsteile verweist, die für diese Nutzergruppe erfahrungsgemäß von besonderer Relevanz sind.

In ähnlicher Weise kann die Orientierung für die Bürgerinnen und Bürger durch eine Strukturierung des Verwaltungsangebots nach Lebenslagen erleichtert werden. Hier wird alternativ oder ergänzend zu der Unterscheidung nach speziellen Rollen nach bestimmten Situationen unterschieden, in denen typischerweise mehrere Kontakte mit verschiedenen Verwaltungen anfallen. Nach Auswahl einer solchen Lebenslage oder Situation können dem Bürger dann unmittelbar Verweise auf die einschlägigen Informationen oder Dienstleistungen in gebündelter Form angeboten werden. Typische Lebenslagen ergeben sich entlang des Lebenszyklus von der Geburt über die Heirat bis zum Tod sowie aus wichtigen Änderungen der persönlichen Verhältnisse, z. B. nach einem Umzug oder Arbeitsplatzwechsel.

**Lebenslagen-
prinzip**

Mit der Gliederung nach Rollen und/ oder Situationen verbinden sich neben dem unmittelbaren Nutzen für die Orientierung im Verwaltungsangebot zwei weitere Effekte: Erstens können die Bürger so auf Informationen oder Dienste hingewiesen werden, die durchaus relevant für sie sind, von denen sie zuvor aber noch gar nichts gewusst haben. Zweitens ermöglicht es gerade das Lebenslagenprinzip, die relevanten Angebote unabhängig von Zuständigkeiten und Organisationsstrukturen zu bündeln.⁸ Dies ist insbesondere bei Behörden übergreifenden Portalen wie www.bund.de oder den entsprechenden Angeboten der Bundesländer von Interesse. Doch auch einzelne Behörden können die Darstellung zu Lebenslagen durch Links auf einschlägige Angebote anderer Behörden komplettieren.

**Gliederung nach
Rollen und/ oder
Situationen**

Zusätzlich zu den thematischen Gliederungen sollte das Angebot durch Namens- und Indexlisten erschlossen werden. Diese Listen sind alphabetisch sortiert und können sich zum einen auf die Namen von einzelnen organisatorischen Einheiten und zum anderen auf die erbrachten Dienstleistungen beziehen. Bürger, die genau wissen, was sie wollen, können über einen solchen Index das Gewünschte schnell und unmittelbar aufrufen. Voraussetzung dafür ist allerdings, dass ein solcher Index sorgfältig erstellt wurde, kontinuierlich gepflegt wird und die Verschlagwortung aus Nutzersicht vorgenommen wird. Wenig hilfreich wäre es z. B., bestimmte Angebote mit Stichpunkten wie „Antrag auf ...“ oder „Information über ...“ zu belegen, auch wenn dies aus Verwaltungssicht eine korrekte Beschreibung der gebotenen Leistung darstellen mag. Statt dessen sollten prägnante und verständliche Begrifflichkeiten gewählt und auch synonym gebräuchliche Bezeichnungen aufgenommen werden. Der Index eines Online-Angebots folgt also im Prinzip den gleichen Regeln wie die Erstellung eines Schlagwortverzeichnisses für ein umfangreiches Buch.

**Namens- und
Indexlisten**

Bürger treten mit unterschiedlichen Gewohnheiten, Wünschen, Orientierungsmustern und Erwartungen an das Web-Angebot einer Verwaltung heran. Um dieser Vielfalt gerecht zu werden, sollten die Bürger zwischen mehreren der genannten Möglichkeiten zur inhaltlichen Erschließung eines Web-Angebots wählen können. Um den inhaltlichen Zugang des Bürgers zum Angebot zu unterstützen,

**Platzieren von
Zusammen-
fassungen**

⁸ Vgl. zur Bündelung von Dienstleistungen auch das Modul „Bewertungskriterien für potenziell online-fähige Dienstleistungen“ (IV A), Abschnitt 7.

empfiehlt es sich ergänzend zu den genannten Orientierungshilfen gerade vor längeren Textpassagen kurze, prägnante Zusammenfassungen zu platzieren. Dies kommt allen Nutzergruppen entgegen, erleichtert es aber insbesondere Benachteiligten (Ältere, Sehbehinderte usw.), sich einen Überblick zu verschaffen.

Generell sollten die Bürgerinnen und Bürger beim Aufrufen einer Verwaltungsseite (und auch im weiteren Verlauf ihres Besuchs im Angebot) sofort die Zugehörigkeit der betreffenden Behörde zur jeweiligen Gebietskörperschaft erkennen können. Diesem Zweck dienen u. a. Wappen, Logos, Farbgestaltung, Schriftwahl und weitere Maßnahmen. Um hier das erforderliche Maß an Einheitlichkeit zu gewährleisten, werden in Styleguides verbindliche Festlegungen getroffen, an denen sich die jeweiligen Behörden orientieren sollen oder müssen. Ferner sollte eindeutig darauf aufmerksam gemacht werden, wo der Zuständigkeitsbereich der betreffenden Verwaltung(en) endet. Dies betrifft insbesondere externe Links, die als solche gekennzeichnet werden sollten, um Missverständnisse zu vermeiden.

Site-Image

2.2.2 Suchmaschine

Bei umfangreichen Web-Angeboten, insbesondere bei so genannten Portalen, ist eine ergonomische Suchmaschine zum Auffinden spezieller Informationen fast schon unverzichtbar. Der Wunsch, mittels Suchmaschine eine Recherche durchzuführen, kann in jeder Phase der Nutzung eines Online-Angebots auftreten. Aus diesem Grund sollte die Existenz einer Suchmaschine auf der Startseite deutlich erkennbar sein. Weiterhin sollte die Suchmaschine von jeder Seite des Online-Angebots aus angesteuert werden können, ohne dass zuvor die Rückkehr zur Hauptseite erforderlich wird.

**Abschnitt 2.2.2
Aufwand 3, Bedeutung 3**

Dabei ist zwischen einer Volltextsuche und einer indexbasierten Suche zu unterscheiden. Die üblicherweise angebotene Volltextrecherche sucht auf allen Seiten nach der eingegebenen Zeichenfolge. Die Eingabe „Auto“ führt dann auch zum „Autogenen Training“, aber nicht zur Kfz-Zulassung. Dies leistet eine indexbasierte Suche, für die alle Seiten mit Schlagworten versehen werden müssen. Ein solcher Schlagwortbestand sollte auch Synonyme beinhalten, sodass „Auto“, „PKW“, „Kfz“ usw. zur gleichen Stelle führen.

**Unterscheidung
von Volltext- und
Indexsuche**

Der Nutzen von Suchmaschinen hängt wesentlich von der Präsentation der Suchergebnisse ab. Eine unkommentierte Auflistung von ein paar hundert Links bringt niemanden weiter. Daher sollte zu jedem gefundenen Dokument ein kurzer Fließtext aufgeführt werden, mit dessen Hilfe der Benutzer die Relevanz des Verweises für seinen Zweck einschätzen kann. Weiterhin sollte die Suchmaschine ein „Ranking“ anbieten, sodass an vorderer Stelle jene Dokumente aufgelistet werden, die der Suchanfrage am meisten entsprechen. Generell aber sollte der Bürger vorgeben können, wie er das Suchergebnis dargestellt haben möchte (Anzahl der Treffer auf einer Seite, Ranking oder andere Sortierungskriterien usw.)

**Präsentation der
Suchergebnisse**

Die leistungsfähigste Suchmaschine nutzt wenig, wenn ihre Funktionsweise nicht hinreichend verdeutlicht wird. Das Hauptaugenmerk richtet sich dabei auf die Erklärung grundlegender Funktionen wie die Formulierung von Suchanfragen und die Beschreibung zusätzlicher Funktionen wie logische Verknüpfungen, Suche nach speziellen Datenformaten usw. Klare und eindeutige Beispiele erleichtern dabei die Verständlichkeit. Generell sollte eine in Verwaltungsseiten integrierte

**Grundlegende
Funktionen erklären**

Suchmaschine möglichst weit gehend den üblichen Bürgergewohnheiten entgegen kommen. Beispielsweise sollte Groß- und Kleinschreibung ignoriert und die Benutzung von Umlauten akzeptiert werden.

TIPPS ZU SUCHMASCHINEN

Bei Auswahl und Integration eines Suchmaschinen-Moduls sollten die nachfolgend aufgeführten Punkte berücksichtigt werden.

Die Benutzungsoberfläche für die Eingabe

- Die Anzahl der Eingabefelder sollte auf ein Minimum reduziert sein, um unnötige Irritationen der Suchenden zu vermeiden.
- Wenn neben der Standard-Suche eine Suchfunktion für Experten angeboten wird, muss diese eindeutig bezeichnet werden, um weniger versierte Benutzer nicht mit zusätzlichen Funktionen zu verunsichern.
- Die verwendeten Buttons sollten mit einem unmissverständlichen Label wie „Suchen“, „Finden“ etc. ausgezeichnet werden.
- Falls die Eingabeformulierung Beschränkungen unterliegt, sollte dies mit einer klaren, kurzen Aufforderung verdeutlicht werden (z. B.: „Bitte nicht mehr als drei Suchbegriffe eingeben.“)

Die Verarbeitung der Eingabe

- Falls möglich, sollte sich die Suchmaschine fehlertolerant zeigen und bei „Verschreibungen“, die zu keinem Ergebnis führen, mögliche Alternativen, d. h. in der Schreibweise ähnliche und häufig vorkommende Begriffe, anbieten.
- Das Eingabefeld sollte bereits aktiviert sein, sodass man nicht extra ins Feld klicken muss.
- Die Eingabe sollte auch durch die Enter-Taste abgeschickt werden können, sodass ein Mausclick auf das Feld „Suchen“ nicht nötig ist.

Die Ausgabe der Ergebnisse

- Die Ergebnisse sollten in einer Liste aufgezeigt werden.
- Die Antwortzeit sollte unter zehn Sekunden liegen. Daher sollte standardmäßig eine nicht zu hohe Trefferzahl pro Seite angezeigt werden. Der Bürger sollte aber wählen können, ob er mehr Ergebnisse präsentiert bekommen möchte.
- Wenn die Ergebnisse in einem neuen Fenster angezeigt werden, sollte dies durch die reduzierte Größe dieses Fensters deutlich gemacht werden.
- Die Ergebnisanzeige sollte eine Rückmeldung über die verwendeten Suchkriterien (z. B. auch wenn Synonyme automatisch in die Suche einbezogen wurden) und über den Bereich geben, in dem gesucht wurde (WWW, Webseiten, Sub-Seiten, vorherige Ergebnismenge).
- Die Anzahl der Treffer sollte angegeben werden.
- Eine Vorsortierung der Liste nach relevanten Ergebnissen wäre wünschenswert (dabei muss die Vorsortierung aber sofort erkennbar sein). Der Bürger

sollte dann eine Umsortierung (z. B. nach Aktualität) vornehmen können.

- Die Ergebnisse sollten übersichtlich gruppiert und nummeriert werden.
- Bei zu vielen Treffern sollten sinnvolle, verständliche und leicht bedienbare Filter angeboten werden.
- Null-Treffer-Meldungen sollten deutlich sichtbar, kurz und verständlich sein. Sie sollten sich deutlich von Seiten mit Trefferanzeigen unterscheiden.

Hilfestellungen und Rückmeldungen

- Hilfestellungen sollten knapp und einfach formuliert werden.
- Sie sollten einfache, leicht verständliche Beispiele beinhalten.
- Fehlermeldungen sollten immer Vorschläge für das weitere Vorgehen beinhalten.
- Nach Abschicken der Suche sollte der Bürger immer eine deutlich erkennbare und verständliche Systemrückmeldung erhalten, damit an jeder Stelle klar ist, wie das System arbeitet und was gerade geschieht.
- Für häufig auftretende Fragen (FAQs: frequently asked questions) sollte eine Liste mit Antworten angeboten werden.

2.2.3 Mehrsprachigkeit

Verwaltungsangebote richten sich in vielen Fällen auch, manchmal sogar ausschließlich an Personen, die eine andere Sprache als Deutsch bevorzugen. Die Beispiele reichen von Touristen oder Investoren, die womöglich überhaupt kein Deutsch verstehen, bis zu deutschen Staatsangehörigen, die Deutsch aber nicht als Muttersprache gelernt haben.

**Abschnitt 2.2.3
Aufwand 2, Be-
deutung 3**

Da der Aufwand, das gesamte Angebot parallel in mehreren Sprachen vorzuhalten, kaum zu bewältigen ist, müssen Prioritäten gesetzt werden. So empfiehlt es sich, zumindest wesentliche Teile der Selbstdarstellung in gängige Welt Sprachen zu übersetzen und darüber hinaus nach Zielgruppen zu differenzieren. Zu denken ist beispielsweise an Übersetzungen ins Türkische, um dem Bedarf der mit 2,4 Millionen Menschen größten in Deutschland lebenden Ausländergemeinschaft gerecht zu werden. Hier sollte von Fall zu Fall entschieden werden, welche Angebote in welche Sprachen übersetzt werden. Da gelegentlich Probleme bei der Übersetzung von Fachtermini auftauchen, ist es empfehlenswert, die Übersetzung durch jemanden anfertigen oder überprüfen zu lassen, der gleichermaßen sprach- und fachkundig ist.

Prioritäten setzen

Zu überlegen wäre weiterhin, wie fremdsprachigen Besuchern der Zugang zum Angebot erleichtert wird. Niemand wird sich durch ein umfangreiches Web-Angebot klicken – in der Hoffnung, irgendwo eine relevante Information in der eigenen Sprache zu finden. Je nach Umfang des fremdsprachig gestalteten Angebotsteils sollten auch die unter 1.2.1 aufgeführten Orientierungshilfen mehrsprachig vorgehalten werden. In jedem Fall aber wird es sich empfehlen, die in anderen Sprachen gehaltenen Seiten über ein Inhaltsverzeichnis zu erschließen. Wurde

**Orientierungs-
hilfen mehrspra-
chig gestalten**

nur ein Teil des gesamten Web-Angebots in die betreffende Sprache übersetzt, sollte im Inhaltsverzeichnis an geeigneter Stelle darauf hingewiesen werden.

2.2.4 Barrierefreiheit

Gerade für Menschen mit Behinderungen bietet das Internet neue Möglichkeiten zur Teilhabe am gesellschaftlichen Leben und zur Integration in die Arbeitswelt.

Dazu ist es aber erforderlich, Internet-Anwendungen auch für Behinderte zugänglich zu machen. Während in der Architektur barrierefreie Zugänge zu Gebäuden und Räumen seit langem als Anforderung bekannt sind, ist das Prinzip der Barrierefreiheit bei der Gestaltung von Internet-Diensten erst seit kurzem ein Thema.⁹

Um diese Entwicklung zu fördern, wurden entsprechende Verpflichtungen für Arbeitgeber und Anbieter in das Sozialgesetzbuch IX und das Behindertengleichstellungsgesetz (BGG) aufgenommen. Seit dem 1. Mai 2002 verpflichtet das „Gesetz zur Gleichstellung behinderter Menschen“ Bundesbehörden u. a. dazu, Webseiten so zu gestalten, dass sie auch von Behinderten genutzt werden können.

Da Behinderungen, insbesondere Mehrfachbehinderungen Menschen sehr unterschiedlich einschränken, können die Barrieren, die im Umgang mit Informationstechnik entstehen, nur grob skizziert werden:

- Blinde Menschen sind darauf angewiesen, dass spezielle Software-Produkte die Bildschirminhalte auslesen können. Da die Informationen zur Navigation und Orientierung nur auditiv aufgenommen werden können, ist es notwendig, dass der Aufbau einer Seite übersichtlich strukturiert und leicht verständlich ist. Weiterhin ist es notwendig, dass das gesamte Angebot über Tastatur bedient werden kann. Insbesondere taub-blinde Menschen sind auf die Nutzung einer Braillezeile angewiesen. Barrieren entstehen insbesondere, wenn Textelemente oder Links als Grafik gestaltet werden und der Text von der Software nicht erfasst werden kann.
- Sehbehinderungen weisen sehr unterschiedliche Ausprägungen auf: einige Sehbehinderte sehen unscharf, teilweise kaum mehr als Hell-Dunkel-Kontraste, aber im gesamten Gesichtsfeld. Einige sehen zwar scharf, aber nur in einem sehr schmalen Tunnel, einige reagieren stark auf unterschiedliche Beleuchtungsverhältnisse oder sind farbenblind.¹⁰ Der Übergang zur Gruppe der Blinden ist fließend. Damit bei diesen sehr unterschiedlichen Fähigkeiten und Möglichkeiten eine maximale Sehfähigkeit erreicht werden kann, wird von Sehbehinderten häufig eine Kombination aus Vergrößerungssoftware und Sprachausgabe genutzt. Sehr wichtig sind in allen Softwareprodukten skalierbare Schriftgrößen und die Möglichkeit zu individueller Farbeinstellung.
- Menschen mit motorischen Beeinträchtigungen wie z. B. spastischen Bewegungseinschränkungen sind in ihrer Feinmotorik behindert. Daher ist meist

Zugänglichkeit für Behinderte

Abschnitt 2.2.4
Aufwand 3, Bedeutung 4

Gesetz zur Gleichstellung behinderter Menschen

Unterschiedliche Bedürfnisse

⁹ Zum Einstieg : <http://www.digitale-chancen.de/barrierefreies-egovernment> sowie <http://www.ftb-net.de/>

¹⁰ Mehr als 8% der männlichen Bevölkerung ist farbenblind.

eine Interaktion mit der Maus oder auch mit der Standardtastatur nicht möglich. Auch Menschen, die ihre Arme und Hände nicht vollständig nutzen können, sind auf Alternativen zu den Standardeingaben angewiesen. Dies können spezielle Tastaturen, Kopfmäuse oder auch Schalter sein.

- Hörgeschädigte Menschen haben mit der Interaktion selbst meist wenig Probleme. Schwierigkeiten treten aber dann auf, wenn Audioangebote und Videos ohne Textversion angeboten werden. Eine weitere Barriere betrifft gehörlose Menschen, deren Muttersprache die Gebärdensprache ist: Die deutsche Sprache ist in diesem Fall eher als Fremdsprache einzustufen, so dass die Verwendung einer möglichst einfachen Sprache wichtig ist.
- Für Menschen mit Lernbeeinträchtigungen sind eine klare einprägsame Seitenstrukturierung, eine einfach handhabbare Navigation und die Verwendung einer möglichst einfachen Sprache von zentraler Bedeutung.

Die Verordnung zur Konkretisierung des BGG enthält als zentralen Bestandteil eine Prüfliste, die der Web-Content-Accessibility-Guideline 1.0 entspricht und von der Web-Accessibility-Initiative, einem Arbeitskreis des W3C (World Wide Web Consortium), entwickelt wurde.¹¹ Die Punkte der Checkliste lassen sich fünf Prinzipien zuordnen:

**Gestaltungsregeln
zur Barriere-
freiheit**

- Erreichbarkeit: Kann ich die Informationen aufnehmen, auch wenn ich z. B. nicht hören oder sehen kann?
- Bedienbarkeit: Ist die Anwendung z. B. auch ohne Maus bedienbar?
- Orientierung und Navigation: Gelingt es mir unmittelbar, die Navigationsmöglichkeiten sinnvoll zu nutzen und mich leicht innerhalb des Angebots zu orientieren?
- Verständlichkeit: Werden die Inhalte einfach formuliert und klar strukturiert angeboten?
- Robustheit: Ist die Kompatibilität mit unterstützenden Hilfsmitteln (assistive tools) gewährleistet?

Beispielsweise sollten folgende Regeln beachtet werden:

- Bei grafischen Links sollte gleichzeitig immer eine alternative Textversion angeboten werden.
- Alt-Tags (alternative Texte) können den Inhalt von Grafiken erklären und sollten auch dann verwendet werden, wenn eine alternative Textversion angeboten wird.
- Falls Menüs z. B. mit Java oder Shockwave erstellt worden sind, sollte parallel dazu eine reine HTML-Variante angeboten werden.
- Zu Grafiken und Tabellen sollten immer Zusammenfassungen in Textform angeboten werden.
- Alle farbige dargestellten Inhalte sollten auch ohne Farbunterscheidungsmöglichkeit lesbar sein.

¹¹ <http://www.w3c.org/WAI/>

Die Umsetzung dieser Prinzipien gelingt besonders einfach, wenn der Fokus in der Informationsdarstellung liegt und für die Realisierung auf Technologien wie HTML und CSS zurückgegriffen wird. Allerdings ist für Transaktionen, die nicht allein über HTML-Formulare zu realisieren sind sondern beispielsweise ein Plug-In benötigen, die barrierefreie Umsetzung wesentlich schwieriger. Insbesondere zur Umsetzung von barrierefreien rechtsverbindlichen Online-Transaktionen (s. 3.3), bei denen elektronische Signaturen zum Einsatz kommen, besteht noch Forschungsbedarf.

Als Hilfestellung zur Überprüfung der Barrierefreiheit von Webseiten bietet CAST (Center for Applied Special Technology) ein Programm namens Bobby an.¹²

Wenn die Orientierung im Web-Angebot ohne jegliche optische Eindrücke allein durch das vorgelesene Wort erfolgen muss, ist eine klare, einprägsame und nachvollziehbare Seitenstrukturierung außerordentlich hilfreich. Dieser Zwang zur durchdachten Struktur ist nicht nur für Sehbehinderte wichtig. Eine verständliche und nachvollziehbare Struktur erleichtert auch Sehenden die Orientierung im Web-Angebot. Zudem stimmt die obige Auflistung einiger wichtiger Gestaltungsregeln zur Barrierefreiheit in weiten Teilen mit jenen Empfehlungen überein, die zur technischen Kompatibilität des Angebots formuliert wurden (s. 2.1.2).

Natürlich hat die barrierefreie Seitengestaltung ihre Grenzen, etwa wenn zur Nutzung bestimmter Funktionalitäten unbedingt ein Plug-In erforderlich ist, das mit einem Screenreader nicht zugänglich ist. Auch wird sich die Umstellung bestehender, komplexer Angebote vielfach als sehr aufwändig herausstellen. In diesen Fällen empfiehlt es sich vermutlich eher, separate Seiten für Blinde anzubieten.

Grenzen der barrierefreien Seitengestaltung

2.2.5 Navigation

Der Bürger sollte leicht und zielorientiert durch das gesamte Web-Angebot navigieren können und jederzeit wissen, in welcher Rubrik er sich gegenwärtig befindet.

Anbieten einer Navigationsleiste

Zu diesem Zweck sollte stets eine Navigationsleiste (gestaltet als Spalte einer Tabelle oder als eigener Navigationsframe) angeboten werden, wobei der aktuelle Bereich jeweils hervorgehoben dargestellt werden sollte. Dieses Navigationsmenü sollte nach Möglichkeit nicht mehr als sieben Rubriken umfassen, damit der Bürger sich schnell einen Überblick verschaffen kann. Ergänzend sollten Verweise zur Startseite und zur Suchmaschine untergebracht werden.

Abschnitt 2.2.5 Aufwand 2, Bedeutung 4

Weiterhin sollten zur Erleichterung der Navigation bei der Seitengestaltung folgende Grundregeln bedacht werden:

Grundregeln zur Navigation

- Sackgassen (dead-ends), aus denen kein Link mehr herausführt, sollten vermieden werden. Der einfachste Weg ist, auf jeder Seite einen Link zur Startseite zu platzieren.

¹² <http://www.cast.org/bobby>

- Seiten sollten kurz gehalten werden, um Scrollen zu vermeiden. Bei längeren Seiten sollten Verweise zum Anfang der Seite eingefügt werden, um schnell wieder zum Seitenanfang zu gelangen.
- Links sollten eindeutig und verständlich bezeichnet werden und Auskunft über den Inhalt der Zielseite geben.
- Das Angebot sollte so strukturiert sein, dass der Bürger schnell zum gewünschten Menüpunkt navigieren kann. Eine Faustregel empfiehlt, dass jede Stelle im Angebot möglichst mit drei „Klicks“ erreichbar sein sollte.
- Für die Seitennutzung mit einem Screenreader (s. 2.2.4) sollte ein Button eingesetzt werden, der die aktuelle Navigation überspringt, damit nicht alle dort aufgeführten Punkte vorgelesen werden, bevor der Übergang zum eigentlichen Inhalt erfolgen kann.

Bei einer Seitengestaltung mit Frames sollte ergänzend bedacht werden, dass die Navigationsfunktionalitäten der Browser nur eingeschränkt verfügbar sind:

**Seitengestaltung
mit Frames**

- Wer schrittweise über den „Zurück-Knopf“ des Browsers zu vorherigen Seiten zurückkehren möchte, muss zuvor ggf. den gewünschten Frame durch Mausklick auswählen.
- Das Anwenden der History-Funktion, um mehrere Seiten zurückzuspringen, ist oftmals nicht möglich.
- Das Bookmarks/ Hinzufügen einzelner Seiten als Favoriten innerhalb des Frame-Sets ist ebenfalls nicht möglich.

Aus diesen Gründen ist es empfehlenswert, bei Verwendung von Frames eigene Navigationsfunktionalitäten bereitzustellen, die unabhängig vom Browser genutzt werden können. Dazu zählen beispielsweise Schaltflächen für „Nächste Seite“ und „Vorhergehende Seite“. Anders als bei den „Vor-“ und „Zurück-Schaltflächen“ der Browser, die stets auf Seiten führen, die zuvor besucht worden sind, handelt es sich dabei um feststehende Verweise auf zuvor festgelegte Dokumentseiten, die dann in der vom Seitenanbieter vorgegebenen Reihenfolge durchgeblättert werden können. Wenn es sich anbietet, sollte auch eine Druckansicht angeboten werden, die den Inhalt eines Frames so aufbereitet, dass er vollständig und übersichtlich ausgedruckt werden kann.

2.2.6 Hilfen

Da selbst bei vorbildlich gestalteten Webseiten gelegentlich Fragen zu Funktionalitäten und Funktionsweisen auftauchen, sollten stets auch Hilfen zur Bedienung des Angebots vorgesehen werden.

**Abschnitt 2.2.6
Aufwand 1, Be-
deutung 4**

Einführungen: Für Gelegenheitsnutzer oder bei aufwändigeren Funktionalitäten sollten überblicksartige Einführungsseiten erstellt werden, auf denen die wichtigsten Voraussetzungen zur Nutzung eines Angebots erklärt werden. Den Gelegenheitsnutzern sollten die technischen Voraussetzungen für bestimmte Funktionalitäten ebenso erklärt werden wie die Struktur des Angebots. Gelegentlich werden selbst häufige Internet-Nutzer von solchen Erklärungen profitieren können, etwa wenn es um die Durchführung komplexer Transaktionen geht.

Kontextsensitive Hilfe: Hier wird die Hilfe zum integralen Bestandteil eines Angebots. Taucht beim Besuch einer Seite eine Frage oder Unklarheit auf, soll es dem Bürger ermöglicht werden, von dieser Position aus unmittelbar eine Hilfe aufzurufen, die sich auf den gerade in Anspruch genommenen Angebotsteil bezieht. Um eine kontextsensitive Hilfe anzubieten, sollte die für die Erarbeitung der Hilfsfunktionen zuständige Stelle eng mit den Seitengestaltern und Programmierern zusammenarbeiten. Beispielsweise müssen Schnittstellen vereinbart werden, um die Verbindung zwischen Hilfe-Dokument und den jeweiligen Teilen des Web-Angebots sicherzustellen. Hilfetexte zu den Eingabefeldern und Auswahlmenüs eines Formulars sollten über Links erreichbar sein. Beim Anwählen des Links würde in diesem Fall auf die entsprechende Stelle in der Online-Hilfe verzweigt, die eine ausführlichere Erläuterung zur betreffenden Position des Web-Angebots liefert.

Fehlermeldungen: Fehlermeldungen sollten verständlich formuliert werden und vor allem einen Vorschlag zur Lösung eines aufgetretenen Problems liefern. Beispielsweise könnte statt „Fehler 404: Datei nicht gefunden“ formuliert werden: „Die von Ihnen aufgerufene Seite konnte nicht gefunden werden. Es besteht die Möglichkeit, dass die von Ihnen gewünschten Informationen nun an anderer Stelle vorgehalten werden. Es empfiehlt sich, eine Stichwortsuche durchzuführen.“

FAQ-Liste: In FAQ-Listen (frequently asked questions) werden häufig wiederkehrende und für das jeweilige Web-Angebot typische Bürgerfragen beantwortet. Eine Quelle zur Ermittlung solcher Fragen sind z. B. die E-Mails, die an den Webmaster eines Angebots gerichtet werden (s. 3.2.1.1).

Hotline: Gerade bei komplexeren Web-Angeboten wird es vorkommen, dass technische Fragen nicht über die Hilfen im Angebot selbst geklärt werden können. Für solche Fälle empfiehlt sich die Einrichtung einer Hotline. Dabei sollte geprüft werden, ob eine solche Hotline nicht mit den von vielen Behörden gegenwärtig entwickelten Call-Center-Dienstleistungen verbunden werden kann. Kontaktdaten und Arbeitszeiten der Hotline sollten schnell aufzufinden sein.

3 Inhaltliche Angebote und Funktionen

Die inhaltlichen Internet-Angebote der öffentlichen Verwaltung lassen sich danach unterscheiden, ob sie primär der Informationsvermittlung, der Kommunikation oder der Abwicklung eines Geschäftsvorfalles (Transaktion) dienen. Die Qualität dieser Angebote bestimmt sich zum einen danach, wie umfangreich und detailliert sie sind. Zum anderen lassen sich für Informations-, Kommunikations- und Transaktionsangebote jeweils spezifische Kriterien für die Nutzungsqualität benennen. Beide Perspektiven werden nachfolgend eingenommen.

3.1 Informationsangebote

Informationsangebote der öffentlichen Verwaltung im Internet sollen die Bürgerinnen und Bürger in die Lage versetzen, sich unabhängig von Sprech- und Öffnungszeiten der Ämter sowie ohne Wege- und Wartezeiten Zugang zu Informationen über Leistungen, Angebote und Arbeit der Behörden zu verschaffen.¹³ Dies ist nicht nur ein Komfortgewinn sondern stärkt auch die Rolle der Bürger im Kontakt mit der Verwaltung, da sie sich selbstständig informieren und gegebenenfalls Details gezielter erfragen können. Informationsangebote im Web sollen den persönlichen Kontakt aber nicht ersetzen sondern ergänzen.

Dem Bürger sollte es möglichst selbst überlassen bleiben, wie er Kontakt mit der Verwaltung aufnimmt. Dabei sind mit den einzelnen Zugangswegen unterschiedliche Vorteile verbunden. Diese können im Fall der Informationssuche beispielsweise wie folgt aussehen: Im persönlichen Kontakt kann der zuständige Verwaltungsmitarbeiter Nachfragen gezielt beantworten. Ein Agent im Call Center kann die gewünschten Informationen ohne lange Wartezeiten geben. Und ein Web-Angebot ermöglicht Zugriff und Erschließung auf umfangreiche Informationsbestände. Dazu ist es allerdings erforderlich, die Möglichkeiten des Mediums gezielt zu nutzen. Beispielsweise können Informationen aus unterschiedlichen Quellen unabhängig von organisatorischen Zuständigkeiten miteinander verknüpft werden. Weiterhin kann auf weiterführende oder thematisch benachbarte Angebote hingewiesen werden, die bei Interesse über einen einfachen Mausklick zu erreichen sind.

Unterschiedliche
Zugangswege

Der Nutzen von Web-Informationsangeboten der öffentlichen Verwaltung hängt sowohl von Umfang und Tiefe des Angebots als auch von der Berücksichtigung wesentlicher Qualitätsmerkmale ab. Die nachfolgenden Hinweise sollen die Entwicklung entsprechender Konzepte unterstützen.

¹³ Vgl. dazu auch Modul „Phase 2 – Strategie“, Aktivität 2.5 „Identifikation notwendiger Infrastruktur-Verfahren“

3.1.1 Umfang und Tiefe

3.1.1.1 Orientierungsinformationen

Nur in den wenigsten Fällen kann davon ausgegangen werden, dass den Bürgerinnen und Bürgern die interne Organisation der Verwaltung und die Verteilung der Zuständigkeiten bekannt sind. Web-Angebote der Verwaltung können hier eine wichtige Orientierungshilfe bieten. Zu diesem Zweck sollten neben grundlegenden Informationen wie Adresse, Telefonnummer und Öffnungszeiten auch Aufgaben, Zuständigkeiten und Ansprechpartner dargestellt werden (s. Beispiel in Abb. 4). Diese Angaben wären dann einheitlich für alle Stellen zu erfassen und sollten, ergänzt um wichtige Schlagworte, in Listenform auch für die Suchfunktionalität verfügbar gemacht werden (s. 2.2.2). Dabei wird es von den Merkmalen der Verwaltungsaufgabe und den zum Bürgerkontakt bestehenden Regelungen abhängen, wie detailliert Zuständigkeiten und Kontaktdaten dargestellt werden. Sind Aufgaben und Zuständigkeiten nicht mit wenigen Worten zu erklären, wird es sich anbieten, die Bürger an eine zentrale Kontaktstelle zu verweisen, die das Anliegen dann gezielt an den zuständigen Mitarbeiter weiterleitet.

Abschnitt 3.1.1.1
Aufwand 1, Bedeutung 3

Da in vielen Fällen der persönliche Kontakt hilfreich bzw. unverzichtbar ist und viele Bürger die Webinformationen auch nur zur gezielten Vorbereitung eines Verwaltungskontakts nutzen, sollten auch Informationen zur Erreichbarkeit geliefert werden. Zu denken ist beispielsweise an die Parkplatzsituation im unmittelbaren Umfeld, die Zugänglichkeit des Gebäudes für Rollstuhlfahrer sowie die Anbindung an den öffentlichen Nahverkehr. Die Stärke des Internets kommt zum Tragen, wenn solche allgemeinen Orientierungsinformationen verknüpft werden mit einer Standortanzeige auf einem Stadtplan-Ausschnitt oder mit Routenplanern für öffentliche Verkehrsmittel.

Weiterhin persönlicher Kontakt

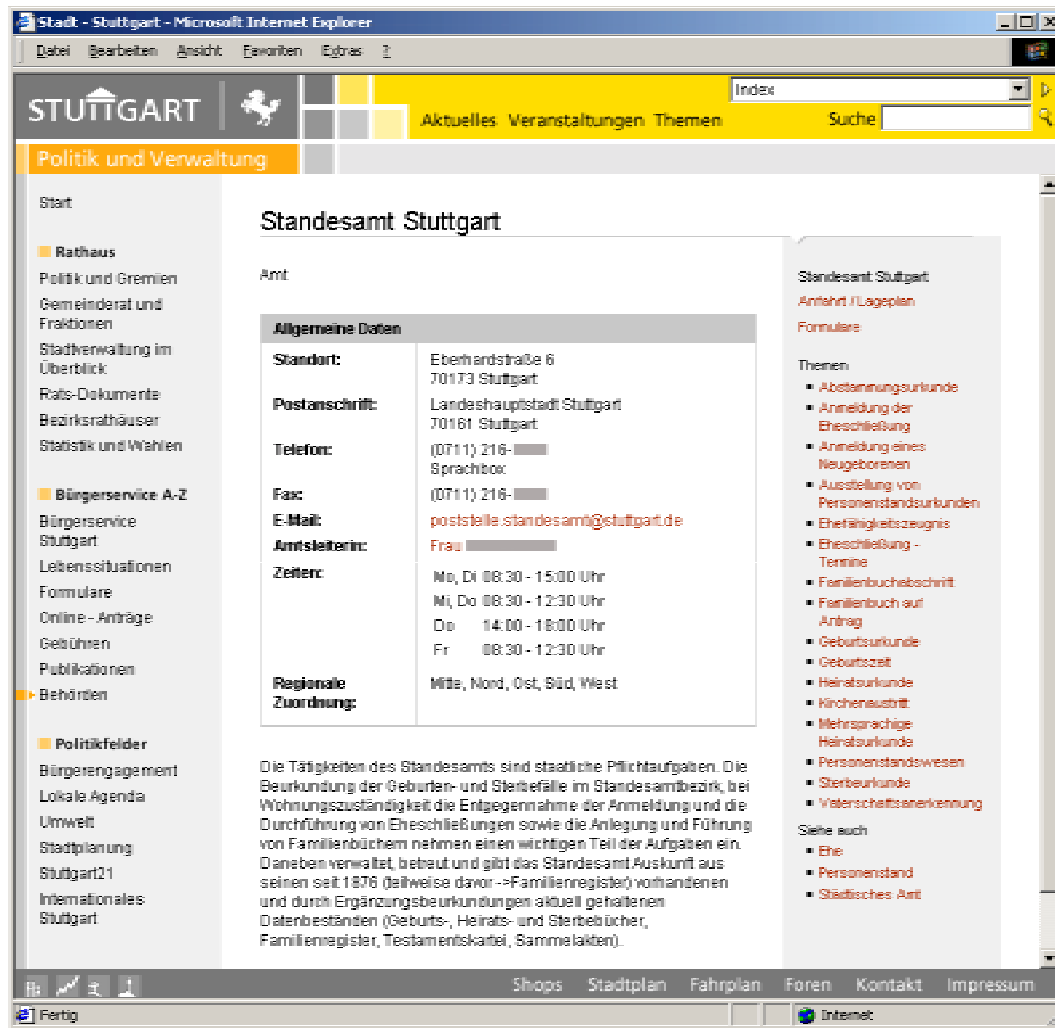


Abb. 4: Beispiel für einen typischen Stammdateneintrag

Hilfreich können weiterhin Informationen zu vorgesetzten und nachgeordneten Behörden sowie zu Verwaltungen mit inhaltlich benachbarten Arbeitsfeldern sein. So können z. B. Bürger, die sich in der Einschätzung der Zuständigkeit geirrt haben, gleich weiterverwiesen werden. Schaut eine Verwaltung bei der Gestaltung ihres Web-Angebots auf diese Weise über den eigenen Tellerrand, ist dies für alle Beteiligten vorteilhaft: Die Bürger ersparen sich erneute Recherchen, und die Verwaltung wird nicht mit Anfragen konfrontiert, für deren Bearbeitung sie gar nicht zuständig ist.

Informationen zu vorgesetzten und nachgeordneten Behörden

3.1.1.2 Informationen zu Verwaltungsaufgaben und -leistungen

Neben den Informationen zur allgemeinen Orientierung erwarten die Bürgerinnen und Bürger detailliertere Informationen zu den jeweiligen Verwaltungsaufgaben und -leistungen. Der konkrete Informationsbedarf bestimmt sich dabei nach dem Anlass des Verwaltungskontakts. Hier lassen sich im Wesentlichen drei Spielarten unterscheiden:¹⁴

Abschnitt 3.1.1.2 Aufwand 2, Bedeutung 4

¹⁴ Klaus Lenk u. a.: Bürgerinformationssysteme. Strategien zur Steigerung der Verwaltungstransparenz und der Partizipationschancen der Bürger, Opladen: Westdeutscher Verlag 1990, S. 28 ff.

- **Verfahrens Anliegen:** Der Bürger will bestimmte Leistungen erlangen (Leistungsanliegen), Eingriffe oder Belästigungen abwehren (Abwehranliegen) oder Veränderungen anregen und Entscheidungen beeinflussen (Partizipationsanliegen).
- **Kontrollanliegen:** Der Bürger will sich allgemein oder aus einem speziellen Eigeninteresse darüber informieren, welche Entwicklungen aktuell im politisch-administrativen System vor sich gehen. Er verfolgt kein eigenes Verfahrens Anliegen, gewünscht wird vielmehr ein gewisser „Durchblick“ über Gesetzesvorhaben, Verfahrensregelungen oder aktuelle Planungen.
- **Informationsanliegen:** Der Bürger fragt nach Informationen, die für die Bewältigung seines Alltags relevant sind (z. B.: Wo liegen die Kindergärten? Gibt es eine Selbsthilfegruppe, die mir weiterhelfen kann?).

An dieser Stelle lassen sich kaum allgemeingültige Empfehlungen für Umfang und Gestaltung des auf die speziellen Leistungen und Aufgaben einer Verwaltung bezogenen Informationsangebots geben. Es sollte aber geprüft werden, welchen Stellenwert die drei Anliegenarten im Kontakt mit den Bürgern erfahrungsgemäß einnehmen und wie das Informationsangebot darauf abgestimmt werden kann (s. Abb. 5).

Verfolgt der Bürger ein Leistungsanliegen, wird er erwarten, dass die zuständigen Stellen benannt sowie Verfahren, Anspruchsvoraussetzungen, Fristen, gegenseitige Rechte und Pflichten usw. beschrieben werden. Je komplexer die der Leistung zugrunde liegenden Rechtsgrundlagen, desto umfangreicher wird die Darstellung im Web ausfallen. Sollte die Möglichkeit zum Formular-Download oder sogar zur Online-Antragstellung bestehen (s. 3.3) sind solche Darstellungen zu Leistungsanliegen erst recht unverzichtbar, um Fehler bei der Antragstellung zu vermeiden. In diesen Fällen sollte das Informations- direkt mit dem Transaktionsangebot verlinkt werden. Bei Abwehranliegen wird in vielen Fällen schon die Benennung der zuständigen Stellen und die Beschreibung des einschlägigen Verfahrens ausreichen, da die Klärung weiterer Details in den meisten solcher Fälle sowieso den persönlichen Kontakt vor Ort oder per Telefon erfordert. Wer bei Planungen und Entscheidungen mitreden will (Partizipationsanliegen), wünscht aktuelle Informationen sowie Verweise auf Mitwirkungsmöglichkeiten (s. 3.2.3). Bei größeren Bauvorhaben können über das Internet z. B. Planungsunterlagen wie Beschreibungen mit Hintergrundinformationen, Kartenmaterial, Pläne, Entwürfe, Fotos usw. zugänglich gemacht werden.

Anliegenarten im Kontakt mit Bürgern

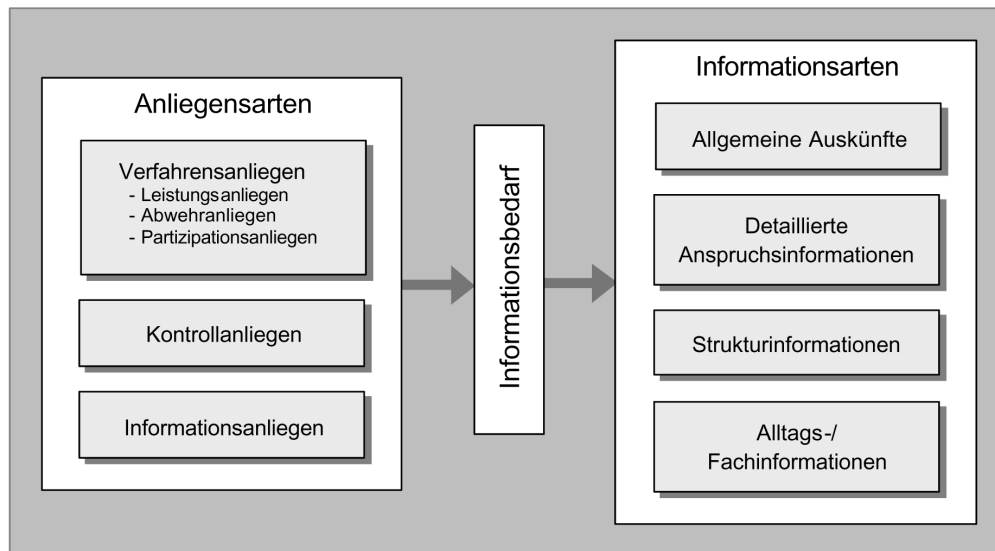


Abb. 5: Bürgeranliegen und Informationsbedarf

Zur Verfolgung von Kontrollanliegen ist es hilfreich, wenn über die allgemeinen Orientierungsinformationen hinaus Darstellungen zur Verwaltungsorganisation und zum Ablauf bestimmter Verfahren angeboten werden. Auch hier könnte es sich z. B. anbieten, über aktuelle Planungen zu informieren oder den Entwurf von Verordnungen ins Netz zu stellen.

Auf die häufigsten Informationsanliegen ist in der Vergangenheit mit Broschüren und Faltblättern reagiert worden. Auch diese Materialien können selbstverständlich übers Internet zugänglich gemacht werden (2.1.1.3). Darüber hinaus sollte aber die Chance genutzt werden, eigenständige Web-Informationsangebote aufzubauen, mit denen wesentlich spezifischer auf die Wünsche der Bürger eingegangen und vor allem auch wesentlich aktueller informiert werden kann. Auf Informationen aus aktuellem Anlass kann schon auf der Startseite hingewiesen werden. Mit einer FAQ-Liste können Antworten zu den häufigsten Fragen gegeben werden, und ein regelmäßiger Newsletter (s. 3.2.2) kann überblicksartig über aktuelle Entwicklungen informieren und auf weiterführende Ausführungen im Web-Angebot hinweisen. Als weiterer Vorteil kommt hinzu, dass viele Informationen für den Abruf via Web nicht einmal selbst aufbereitet werden müssen, ein einfacher Link auf entsprechende Angebote auf anderen Seiten genügt. Damit wird es beispielsweise selbst der kleinsten Verwaltung ermöglicht, die in ihrem Bereich einschlägigen gesetzlichen Vorschriften online abrufbar zu machen.

3.1.2 Anforderung von Informationsmaterial

Ergänzend zu den direkt auf den Internetseiten bereitgestellten Informationen können insbesondere umfangreichere (Broschüren, Ratgeber) oder häufiger benötigte Materialien (Terminübersichten, Merkblätter, Gebärentabellen usw.) auch zum Download (Herunterladen) auf den lokalen Rechner angeboten werden. Dabei sollten weit verbreitete, möglichst plattformunabhängige Dateiformate (wie z. B. PDF) gewählt werden.¹⁵ Gerade bei umfangreicheren Materialien wird sich

Abschnitt 3.1.2
Aufwand 2, Bedeutung 4

¹⁵ Vgl. auch dazu die im Rahmen von SAGA formulierten Empfehlungen (s. Fußnote 2).

der Rückgriff auf ein Plug-In anbieten, mit dem sichergestellt werden kann, dass die Formatierungen und Aufteilungen des Originals beim Ausdruck mit einem womöglich vollkommen anders konfigurierten System erhalten bleiben. Um auch denjenigen, die nicht mit einem solchen Plug-In arbeiten können oder wollen, den Zugriff zu erleichtern, sollte Informationsmaterial auch mit einem entsprechenden Online-Formular über den Postweg angefordert werden können.

Im Einzelfall kann es beim Vertrieb von Materialien erforderlich werden, den in § 312c BGB (vormals § 2 Fernabsatzgesetz) festgeschriebenen Pflichten zur Unterrichtung der Verbraucher zu entsprechen. Danach sind beispielsweise klare und verständliche Informationen über wesentliche Merkmale der Ware oder Dienstleistung, den Zeitpunkt des Zustandekommens eines Vertrages, Preise sowie anfallende Liefer- und Versandkosten erforderlich. In § 312d BGB sind Widerrufs- und Rückgaberecht geregelt (siehe auch Modul „E-Commerce im E-Government“ (IV A)).

Unterrichtung bei Fernabsatz

3.1.3 Nutzungsqualität

Damit die Bürgerinnen und Bürger die ihnen über das Internet verfügbar gemachten Informationen auch tatsächlich in ihrem Sinne nutzen können, müssen diese nicht nur korrekt und aktuell sondern auch für Laien verständlich sein. Diese Anforderungen zu erfüllen, ist nicht immer einfach.

3.1.3.1 Korrektheit und Vertrauenswürdigkeit des Angebots

Die Informationsangebote zu den einzelnen Aufgabengebieten sollten von den fachlich zuständigen Verwaltungsmitarbeitern verantwortet und inhaltlich gepflegt werden, da nur sie über das für eine korrekte Darstellung erforderliche Fachwissen verfügen. Ungenauigkeiten oder Fehler können das gesamte Web-Angebot als nicht vertrauenswürdig diskreditieren, so dass bei der Erstellung und Pflege von Informationstexten sorgfältig gearbeitet werden sollte.

Abschnitt 3.1.3.1
Aufwand 1, Bedeutung 4

Diese inhaltliche Betreuung durch die zuständige Fachverwaltung sollte durch entsprechende Angaben auf den Seiten auch dokumentiert werden. Erstens verstärkt dies die Verpflichtung der Mitarbeiter, die Seiten in ihrem Zuständigkeitsbereich aktuell zu halten. Zweitens kann die dokumentierte Einbeziehung von Sach- und Fachkompetenz die Vertrauenswürdigkeit eines Web-Angebots aus Sicht der Bürgerinnen und Bürger stärken.

Die Vertrauenswürdigkeit eines Angebots wird weiterhin davon beeinflusst, ob die Seiten auf Rechtschreib-, Grammatik- und Tabellenformatierungsfehler und ungültige Links geprüft worden sind bzw. regelmäßig überprüft werden. Ist dies nicht der Fall, werden viele Bürger von der mangelnden Sorgfalt bei der Form auf eine eben solche beim Inhalt schließen.

Rechtschreibung und Grammatik

3.1.3.2 Verständlichkeit

Zur Verständlichkeit kann zum einen eine ansprechende optische Aufbereitung beitragen, indem z. B. Überschriften, wichtige Schlagworte und Kernaussagen hervorgehoben werden. Dabei sollte beachtet werden, dass Textinformationen nicht als Grafik dargestellt werden, da sie sonst von Screenreadern und Suchmaschinen nicht mehr als solche erfasst werden können (s. 2.2). Zum anderen bedürfen komplexe Informationen einer inhaltlichen Aufbereitung, damit sie bei Verbreitung übers Web vom Bürger aufgenommen und verstanden werden können. Insbesondere empfiehlt es sich, die wesentlichen Fakten kurz und knapp darzustellen und gegebenenfalls auf weitergehende Informationen zu verweisen und zu verlinken. Sollten sich längere Texte nicht vermeiden lassen, erleichtern Zwischenüberschriften und Zusammenfassungen die Informationsaufnahme.

**Abschnitt 3.1.3.2
Aufwand 3, Bedeutung 3**

Der Textstil sollte sich den Bedürfnissen der Bürger anpassen, lange Schachtelsätze also ebenso vermieden werden wie „Amtsdeutsch“. Zur korrekten Beschreibung von Ansprüchen, Verfahren, Sachverhalten usw. wird sich die Verwendung von Fachtermini häufig nicht vermeiden lassen. In diesen Fällen sollten Begriffe, die nicht der Alltagssprache entstammen, einführend erklärt werden. Alternativ oder ergänzend zu Erklärungen im Text oder in einer Fußnote bietet sich die Erstellung eines Glossars an, auf das die Informationstexte dann mit einem Link verweisen können. In einem solchen Glossar besteht wiederum die Möglichkeit auf weitergehende Informationen, Rechtsgrundlagen usw. zu verlinken.

Kein „Amtsdeutsch“

Fachbegriffe, die nichts mit dem Thema der jeweiligen Seite zu tun haben, sollten soweit wie möglich vermieden werden. Bei der Verwendung von Begrifflichkeiten mit stark regionalem Einschlag sollte darauf geachtet werden, dass ein Text auch für Seitenbesucher von außerhalb verständlich bleibt und keine Missverständnisse hervorgerufen werden.

Vermeiden von Fachbegriffen

Zur Verständlichkeit eines Informationsangebots gehört es auch, dass sich der Bürger bei Bedarf bestimmte Funktionalitäten, z. B. das Herunterladen einer Broschüre oder das Laden eines Plug-Ins, erklären lassen kann. Dabei sollte EDV-Jargon so weit wie möglich vermieden werden. Für die Erläuterung immer wiederkehrender und nicht zu vermeidender Fachbegriffe bieten sich ähnliche Lösungen an wie bei den Fachtermini der Verwaltung. Weiterhin sollte bei längeren Prozeduren, etwa bei Datenbankabfragen, eine Fortschrittsanzeige die Tätigkeit des Systems dokumentieren und dem Bürger verdeutlichen, was gerade passiert.

Erläuterungen zu Downloads

Zur Erfüllung all dieser Anforderungen empfiehlt sich in der Regel die enge Abstimmung zwischen den fachlich zuständigen Stellen und der Web-Redaktion bzw. der für Presse- und Öffentlichkeitsarbeit zuständigen Organisationseinheit(en). Dabei sollten erstere für die fachliche Richtigkeit und letztere für die verständliche Darstellung und die Einheitlichkeit verantwortlich sein.

3.1.3.3 Aktualität

Ein eigenständiges Qualitätskriterium, das aber auch direkten Einfluss auf die Vertrauenswürdigkeit eines Angebots besitzt, ist die Aktualität der Informationen. Veraltete Daten in einer massenhaft gedruckten Broschüre mögen viele Bürger in der Annahme, dass diese eben erst bei der nächsten Neuauflage beseitigt werden,

**Abschnitt 3.1.3.3
Aufwand 3, Bedeutung 4**

noch verzeihen. Es ist aber gerade ein wesentliches Charakteristikum des Internets, dass Informationen mit vergleichsweise geringem Aufwand aktuell gehalten werden können. Veraltete Angaben werden hier wesentlich eher als bei anderen Medien als Ausdruck mangelnder Sorgfalt gewertet. Aus diesem Grund sollten die fachlich zuständigen Betreuer der Seiten diese regelmäßig auf ihren Aktualisierungsbedarf hin überprüfen. Diese Sorgfaltspflicht sollte externe Seiten, auf die verlinkt wird, einbeziehen. Ein externes Angebot mag zum Zeitpunkt der ersten Verlinkung eine hilfreiche und weiterführende Ergänzung zu eigenen Inhalten dargestellt haben. Werden die dortigen Informationen aber nicht auf dem aktuellen Stand gehalten, fällt dies früher oder später auf das eigene Angebot zurück – etwa wenn widersprüchliche Angaben auftauchen und die Bürger sich fragen, welche Information denn nun die richtige ist.

Um Aktualität zu demonstrieren, empfiehlt es sich, auf jeder Seite einen Hinweis anzubringen, wann die letzte Aktualisierung vorgenommen wurde. Da in vielen Fällen gar keine regelmäßigen Aktualisierungen anfallen, kann dort ersatzweise das Datum der letzten, routinemäßigen Durchsicht angezeigt werden. Denn ein mehrere Jahre zurückliegendes Aktualisierungsdatum wird viele Bürger verunsichern – und zwar auch dann, wenn sich bei den geschilderten Sachverhalten seit Jahren keine inhaltlichen Änderungen mehr ergeben haben.

Aktualitätshinweise setzen

Für besonders aktuelle und wichtige Nachrichten können als zusätzliches Gestaltungselement auch Newsticker (über den Bildschirm laufender Text mit wechselndem Inhalt) eingebaut werden. Bei der Verwendung solcher Extras sollte aber sparsam vorgegangen werden, da sie eine Seite schnell überladen, die Übersichtlichkeit beeinträchtigen und von manchen Bürgern aufgrund der verfügbaren technischen Konfiguration gar nicht gelesen werden können (auf die Verwendung von aktiven Inhalten wird später unter 4.3 noch eingegangen). Sollte aber ein Newsticker verwendet werden, sollte dieser den damit dokumentierten Anspruch von Tages-, wenn nicht sogar Stundenaktualität auch einlösen.

Newsticker

3.2 Kommunikationsangebote

Neben der Bereitstellung von Informationen durch die Verwaltung und den Abruf durch die Bürgerinnen und Bürger dient das Internet auch der beidseitigen Kommunikation. Dies betrifft insbesondere die Nutzung von E-Mail als Alternative oder Ergänzung zu herkömmlichen Kommunikationsformen wie Briefen, Telefonaten oder Faxen. Mit Newslettern und Mailing-Listen sowie mit Online-Diskussionsangeboten entstehen weitere neue Formen der Kommunikation zwischen Verwaltungen und Bürgern.

3.2.1 E-Mail

3.2.1.1 Umfang und Tiefe

Die Anlässe zur Kontaktaufnahme per E-Mail werden sich in der Regel nicht wesentlich von den Gründen unterscheiden, warum bislang Briefe geschrieben, Tele-

**Abschnitt 3.2.1.1
Aufwand 2, Bedeutung 4**

fonate geführt oder Faxe geschickt worden sind. Eine Besonderheit der Kontaktaufnahme via E-Mail besteht allerdings darin, dass eine E-Mail schneller geschrieben und geschickt ist als ein Fax oder Brief und dass die Kommunikation unpersönlicher erfolgt als am Telefon oder bei einem persönlichen Gespräch. Die Kombination dieser beiden Sachverhalte führt in der Regel zu einer Intensivierung der Kommunikation zwischen Verwaltung und Bürgern, indem viele An- und Nachfragen per E-Mail eingehen. In Teilen hat es eine Verwaltung aber auch selbst in der Hand, die Anzahl eingehender E-Mails dadurch zu begrenzen, dass ein gut gestaltetes, umfangreiches und aktuelles Informationsangebot viele Fragen klärt, ohne dass persönlich kommuniziert werden muss. Informations- und Kommunikationsangebote stehen also in enger Beziehung zueinander.

Abhängig von Behördenaufgabe und -größe kann die E-Mail-Kommunikation ganz unterschiedlich organisiert werden. In kleineren bis mittelgroßen Behörden, in denen die Aufgaben und Zuständigkeiten klar verteilt sind, kann es sich anbieten, mit den für ein bestimmtes Anliegen zuständigen Mitarbeitern direkt per E-Mail Kontakt aufzunehmen. In anderen Fällen, etwa wenn die Nennung der zuständigen Mitarbeiter bewusst vermieden werden soll, können E-Mails an die zuständige Organisationseinheit adressiert werden. Und in wieder anderen Fällen wird es sich anbieten, nach dem Vorbild der heutigen Poststellen, einen zentralen E-Mail-Eingang (elektronische Poststelle) zu verwalten, von der aus die eingehende elektronische Post an die zuständigen Einheiten oder Mitarbeiter weitergeleitet wird. Im Zuge einer Prozessoptimierung innerhalb der Behörde zum Zweck der Bereitstellung von E-Government-Dienstleistungen sollte die Nachbildung der Behördenstruktur in eine „virtuelle Behörde“ mit Organisations- oder Funktionspostfächern geprüft werden.

Organisation der E-Mail-Kommunikation

Die Möglichkeit, eine E-Mail an die elektronische Poststelle einer Verwaltung zu richten, stellt aus Sicht der Bürgerinnen und Bürger sicher eher eine Mindestanforderung an das Web-Angebot einer Verwaltung dar. Es ist zu vermuten, dass viele eine zielgenauere Adressierung vorziehen würden. Hier ist eine sorgfältige Abwägung zwischen den Interessen der Bürger und denen der Verwaltung empfehlenswert.

Neben der Möglichkeit, sich mit einer speziellen fachlichen Nachfrage per E-Mail an die Verwaltung zu wenden, sollte es auch möglich sein, auf diesem Weg mit der redaktionell und gestalterisch für das Web-Angebot zuständigen Stelle (Webmaster) Kontakt aufzunehmen. Den Gestaltern eines Web-Angebots können per E-Mail Fehler gemeldet und Verbesserungsvorschläge unterbreitet werden, was der Qualität des Gesamtangebots zugute kommt.

Kontaktaufnahme mit dem Webmaster

3.2.1.2 Nutzungsqualität

Wer sich per E-Mail an seine Verwaltung wendet, wird eine deutlich schnellere Rückmeldung als auf dem Postweg erwarten. Insofern stellt die Kommunikation per E-Mail sicherlich neue Anforderungen an die Reaktionsfähigkeit der öffentlichen Verwaltung. Diese Reaktion muss nicht unbedingt in einer abschließenden Antwort bestehen – dies wird in den meisten Fällen auch gar nicht zu leisten sein. Wichtig ist aber, dass der Eingang der Nachricht bestätigt und bei aufwändigeren Anfragen die Bearbeitung innerhalb einer gewissen Frist in Aussicht gestellt wird.

Antwortzeiten der Verwaltung

Abschnitt 3.2.1.2 Aufwand 3, Bedeutung 2

Es wäre als Ausdruck hoher Serviceorientierung zu werten, wenn eine Verwaltung auf ihrer Webseite zusichert, dass Bürger auf ihre E-Mail-Anfragen innerhalb einer garantierten Frist eine Antwort erhalten. In einfachen Fällen sollte sie gleich die erwünschte Auskunft beinhalten, in allen anderen Fällen zumindest den Eingang der Nachricht bestätigen und gegebenenfalls über die weitere Bearbeitung informieren (Zuständigkeit, voraussichtliche Bearbeitungsdauer usw.). Eine solche erste Antwort sollte nicht länger als zwei Tage auf sich warten lassen.

Die Qualität der E-Mail-Kommunikation hängt natürlich wesentlich davon ab, dass korrekte und aktuelle Informationen gegeben werden. Darüber hinaus wird es sicherlich positiv aufgenommen, wenn auch Hinweise auf weiterführende Informationen im Web gegeben würden. Selbst Standardantworten zu häufig nachgefragten Themen können solche zusätzlichen Hinweise enthalten und somit auf vergleichsweise einfache Weise einen hohen Serviceanspruch dokumentieren.

Korrekte und aktuelle Informationen

Für die Bürger sollte erkennbar sein, ob ihre Anfrage von einer zentralen Poststelle oder der zuständigen Organisationseinheit empfangen wird. Für Postfächer von Organisationseinheiten sollten Vertretungsregelungen getroffen werden, damit auch bei Urlaub oder Krankheit eine zügige Reaktion auf eingehende E-Mails sichergestellt ist. Sollte dies nicht möglich sein, empfiehlt es sich, dass nach Eingang einer Mail automatisch eine Antwort generiert wird, die den Bürger über mögliche Verzögerungen informiert und einen Ansprechpartner für dringende Fälle benennt.

Sofern dies möglich ist, sollte dokumentiert werden, welche Fragen besonders häufig per E-Mail gestellt werden. Dies kann wertvolle Hinweise auf einen Informationsbedarf liefern, der durch das Web-Angebot in seiner bestehenden Form noch nicht befriedigt wird. Die Behebung dieses Informationsdefizits wird im Idealfall wiederum zu einer Reduzierung der individuell zu beantwortenden E-Mail-Anfragen und damit zu einer gewissen Arbeitsentlastung führen.

Dokumentieren von häufig gestellten Fragen

3.2.2 Newsletter

Ergänzend zum Informationsangebot, in dem die Bürgerinnen und Bürger recherchieren, kann das Internet als Kanal zur aktiven Information der Bürgerinnen und Bürger durch die Verwaltung genutzt werden. Dazu bieten sich Newsletter zu bestimmten Themenbereichen an, die ihre Abonnenten per E-Mail über aktuelle Ereignisse informieren. Wer den Bezug eines Newsletters wünscht, trägt in ein entsprechendes Web-Formular u. a. die E-Mail-Adresse ein, zu der die Zustellung erfolgen soll. Ebenso einfach ist es, einmal abonnierte Dienste wieder abzubestellen: Meist reicht eine E-Mail mit einem entsprechenden Vermerk in der Betreffzeile oder eine leere Mail an eine separate Adresse (no-mail@...), um sich aus einem Verteiler wieder auszutragen.

Abschnitt 3.2.2 Aufwand 3, Bedeutung 2

Newsletter von Verwaltungen werden meist von einer Stelle aus redaktionell betreut und mit zugelieferten Inhalten von unterschiedlichen Teilen der Verwaltung gefüllt. Verwaltungen, die einen Newsletter anbieten (möchten), sollten u. a. folgende Punkte beachten:

- Ein Newsletter sollte niemals unaufgefordert zugesendet, sondern immer nur nach einer empfängerseitigen Willensbekundung zugesandt werden.

- Absenderadresse und Betreffzeile sollten selbsterklärend sein, damit die Empfänger auf den ersten Blick sehen können, dass es sich bei der eingegangenen E-Mail um den von ihnen bestellten Newsletter handelt.
- Die Anzeige der E-Mail-Adressen der Empfänger sollte im E-Mail-Kopf unterdrückt werden, um zu verhindern, dass sie von Dritten ohne Einwilligung der Adressinhaber für Werbezwecke genutzt werden. Selbstverständlich sollte ein solcher Newsletter-Verteiler auch nicht an Dritte weitergegeben oder intern für andere Zwecke verwendet werden.
- Vom Aufbau her sollten gerade bei längeren Newsletter-Ausgaben zu Beginn die Überschriften der einzelnen Meldungen, evtl. verbunden mit einer sehr knappen Zusammenfassung, aufgeführt werden. Dies ermöglicht es den Empfängern, sich schnell einen Eindruck zu verschaffen, ob für sie etwas Interessantes enthalten ist. Generell sollten die Meldungen eher knapp gehalten werden, gegebenenfalls empfiehlt sich der Verweis auf weiterführende Darstellungen im Web. In diesem Fall sollte die entsprechende Seite direkt über einen Link im Newsletter erreichbar sein.
- Jeder Newsletter sollte am Ende einen Hinweis enthalten, wie das Abonnement durch den Empfänger beendet werden kann.
- Von Fall zu Fall können auch Beiträge in älteren Newsletter-Ausgaben von Interesse sein. Zu diesem Zweck sollte im Web-Angebot der Verwaltung ein Archiv mit Inhaltsübersicht und Suchfunktion zur Verfügung gestellt werden.

3.2.3 Mailinglisten

Im Unterschied zu Newslettern dienen Mailinglisten der multilateralen Kommunikation, indem E-Mails, die an eine solche Liste geschickt werden, an alle auf dem Listenverteiler eingetragenen E-Mail-Adressen weitergeleitet werden. Dies kann völlig automatisiert oder vermittelt durch einen Redakteur geschehen, der beispielsweise darauf achten könnte, dass über die Mailingliste keine beleidigenden oder anderweitig strafbaren Inhalte verbreitet werden. Mailinglisten ermöglichen Diskussionen zwischen Verwaltung und Bürgern ebenso wie den Gedankenaustausch der Bürger untereinander. Sie werden meist zu speziellen Themen eingerichtet. Im Bereich der öffentlichen Verwaltung könnten auf diese Weise beispielsweise Planungs- oder Gesetzgebungsvorhaben diskutiert werden.

Die Qualität einer Mailingliste hängt stark von der Disziplin aller Beteiligten ab, nur die Mitteilungen zu versenden, die auch für viele Adressaten der Liste von Interesse sind. Werden hingegen über die Liste Diskussionen zwischen einzelnen Teilnehmern geführt, wird das Interesse der übrigen Abonnenten schnell sinken. Eine Verwaltung als Veranstalter einer Mailingliste kann da nur begrenzt einwirken. In vielen Fällen bietet sich daher die Diskussion in moderierten Foren an, da hier durch Moderatoren strukturierende und zielführende Unterstützung erfolgen kann und zudem ein leichter Zugriff auf zurückliegende Beiträge möglich ist.

Abschnitt 3.2.3
Aufwand 2, Bedeutung 1

Disziplin der Teilnehmer

3.2.4 Diskussionsforen

Diskussionsforen bieten den Bürgern die Möglichkeit, untereinander und mit der Verwaltung über bestimmte Themen und Fragen zu diskutieren. Im Unterschied zu Mailinglisten werden die Foren über das Web-Angebot der Verwaltung aufgerufen, die Beiträge der Teilnehmer also nicht per E-Mail versandt. In Foren können ganz unterschiedliche Themen gleichzeitig diskutiert werden, allerdings empfiehlt sich eine nachvollziehbare thematische Strukturierung. Ausgehend von der obersten Ebene, in denen eine Themenübersicht angeboten wird, sollte eine Gliederung nach spezielleren Themen und Fragestellungen („Wurzelforen“) erfolgen. Von dort aus kann nach Einzelaspekten gegliedert werden („Zweigforen“), zu denen dann die Diskussionsbeiträge – meist über ein spezielles Eingabeformular – verfasst werden können. Die einzelnen Beiträge werden dann auf dem Webserver der Behörde gespeichert und können von den nachfolgenden Besuchern der Internetseite gelesen werden. Anschließend können Antworten geschrieben oder eigene Meinungen oder Fragen erörtert werden, indem eine weitere Nachricht eingegeben wird, die wiederum auf dem Webserver gespeichert wird. So kann sich eine längere Diskussion ergeben, die archiviert bleibt und jederzeit nachvollzogen werden kann.

Abschnitt 3.2.4
Aufwand 4, Bedeutung 2

Manche Diskussionsforen dienen dem thematisch offenen Austausch der Bürgerinnen und Bürger untereinander, ohne dass Themen vorgegeben werden oder ein Moderator strukturierend eingreift. Solche Angebote finden sich gelegentlich in Kombination mit „Schwarzen Brettern“, in denen Kleinanzeigen jeglicher Art aufgegeben werden können. Etwas stärker strukturiert sind Foren, in denen vom Seitenanbieter bestimmte Themen zur Diskussion vorgegeben werden, in die sonst aber nicht stärker eingegriffen wird. Solche Kommunikationsfunktionalitäten sollten nur angeboten werden, wenn die Frequentierung eines Web-Angebots und/ oder die Aktualität einschlägiger Themen eine gewisse Teilnahme erwarten lassen. Weiterhin sollte der Seitenanbieter die eingegangenen Beiträge regelmäßig durchsehen, um zu verhindern, dass über sein Forum strafbare Inhalte verbreitet werden, für die er ansonsten haftbar gemacht werden kann (s. 6.1). Es muss dem Seitenanbieter also möglich sein, solche Beiträge zu entfernen. Um sich nicht dem Vorwurf der ungerechtfertigten Zensur auszusetzen, sollte ein solcher Schritt an der jeweiligen Stelle begründet werden.

Schwarze Bretter

Neben solchen offenen und weit gehend der nutzerseitigen Selbstorganisation überlassenen Kommunikationsangeboten können zu speziellen Themen, etwa Planungs- oder Gesetzgebungsvorhaben, moderierte Foren angeboten werden. Solche Diskussionsforen werden meist eingebunden in ein umfangreiches Angebot, das den Bürgern vielfältige Informationen zum Diskussionsgegenstand (Textentwürfe, Pläne, Hintergrundinformationen usw.) zur Verfügung stellt. Häufig sind derartige Aktivitäten im Web auch eingebunden in anderweitige Aktivitäten zur Bürgerbeteiligung. Diskussionen und Resultate solcher themenbezogenen Foren bieten Gelegenheit, im Entscheidungsprozess der eigenen Position Gehör zu verschaffen und evtl. sogar Einfluss auf politische Entscheidungsprozesse zu nehmen. Sie erheben also Anspruch auf einen gewissen Grad der Verbindlichkeit – und sei es auch nur, dass die Diskussionen protokolliert und den Entscheidungsträgern zur Verfügung gestellt werden.

Moderierte Foren

Bei der Bürgerbeteiligung via Web handelt es sich um ein für Verwaltungen wie Bürger vergleichsweise neues Angebot. Inzwischen kann auf erste Erfahrungen aus Projekten¹⁶ aufgebaut werden:

- Solche Diskussionsforen sollten zeitlich befristet angeboten werden, um den Aufwand überschaubar zu halten und auf ein konkretes Ergebnis hinzuarbeiten.
- Zur Strukturierung der Diskussion und zur kontinuierlichen Betreuung des Forums sollte ein Moderator bzw. ein Moderatorenteam engagiert werden, das sich den Diskutanten auch namentlich vorstellt. Die Moderatoren können Fragen aufwerfen, schlichten, erläutern, Beiträge zusammenfassen, neu gruppieren usw. Sie sind letztlich auch dafür zuständig, nach Abschluss des Verfahrens die Ergebnisse zusammenzutragen und den Entscheidungsträgern zur Verfügung zu stellen.
- Es sollten Diskussionsregeln formuliert und vorgegeben werden, um Konflikte vermeiden bzw. regeln zu können.
- Durch die aktive Beteiligung der Fachleute aus der Verwaltung können auftretende Fragen schnell und kompetent geklärt werden, wodurch sich die Qualität der Diskussionen verbessern kann.
- Neu eingeführte Themen sollten vom Moderator mit einem kurzen Beitrag eingeführt und gegebenenfalls durch Hinweise auf grundlegende und erläuternde Materialien ergänzt werden.
- Der Diskussionsverlauf sollte in regelmäßigen Abständen zusammengefasst und ggf. neu strukturiert werden. Je nach Verlauf können diese Foren in unregelmäßigen Abständen geschlossen (falls lange nicht mehr besucht oder Thema nicht mehr aktuell) bzw. erweitert werden.
- Sollten die Moderatoren Änderungen an Beiträgen vornehmen, um z. B. ein Statement zwei unterschiedlichen Zweigforen zuzuweisen, sollte dies dargestellt und begründet werden. Dies gilt noch verstärkt, wenn Beiträge wegen strafbarer Inhalte gestrichen werden.
- Bei passender Gelegenheit könnten die Diskussionsangebote durch Abstimmungen (z. B. um ein Meinungsbild zu erzeugen) oder Chats mit Experten und/ oder Politikern ergänzt werden. Auf diese Weise können Attraktivität und Ernsthaftigkeit des Angebots unterstrichen werden.

¹⁶ Beispielsweise hat das Bundesministerium des Innern (BMI) ein umfangreiches Forum zur Diskussion technischer Standards im E-Government eingerichtet (<http://www.bund.de/saga>). Zuvor war vom BMI bereits Mitte 2001 der Entwurf zum Informationsfreiheitsgesetz des Bundes zur Diskussion gestellt worden (<http://www.staat-modern.de/bmiphorum/list.php?f=8>). Weiterhin hat die Stadt Esslingen im Rahmen des vom Bundesministerium für Wirtschaft und Technologie geförderten Städtewettbewerbs MEDIA@Komm die Planungen zu einem Neubaugebiet online diskutieren lassen sowie ein Online-Bürgerforum eingerichtet (<http://forum.esslingen.de/>). Eingebunden in das EU-Projekt E.D.E.N. (Electronic Democracy European Network) hatten auch Bewohner des Bremer Stadtteils Horn-Lehe die Möglichkeit, online über die zukünftige Entwicklung ihres Wohnumfelds zu diskutieren (<http://www.horn-lehe.de>).

- Um eine breite Beteiligung zu erreichen, sollte aktiv Werbung für das Angebot gemacht werden.
- Um den Eindruck einer „Alibiveranstaltung“ zu vermeiden, sollte darüber informiert werden, wie mit den Anregungen und Diskussionsergebnissen verfahren wird. Zusätzlich sollte die Möglichkeit geschehen, dass die Bürger (z. B. via E-Mail) über das weitere Verfahren informiert werden oder sogar eine Reaktion auf ihre jeweiligen Beiträge erhalten.

Umstritten ist, welche Art der Registrierung den Diskussionsteilnehmern abverlangt werden soll. Einerseits könnte der Wunsch nach größerer Sachlichkeit für eine Anmeldung mit Vor- und Nachnamen sprechen. Andererseits sind die Hemmschwellen zur Beteiligung sicherlich geringer, wenn die Beteiligung mit einem frei gewählten Pseudonym („Nickname“) ermöglicht wird. Bislang vorliegende Erfahrungen deuten darauf hin, dass die Diskussionsqualität auch bei anonymisierten Beiträgen ein gutes Niveau erreichen kann. Das Lesen der Beiträge sollte grundsätzlich ohne vorherige Registrierung möglich sein.

Registrierung der Teilnehmer

Um auch Gelegenheitsnutzern die aktive Teilnahme an einer Online-Diskussion zu ermöglichen, sollte die Benutzeroberfläche möglichst einfach und selbst erklärend gestaltet sein. Die wesentlichen Funktionalitäten sollten einführend kurz erklärt und evtl. durch Beispiele erläutert werden. Ergänzend sollte eine Hilfefunktion verfügbar sein, die zumindest bei den häufigsten Fragen und Problemen weiterhilft.

Einfache Benutzeroberfläche

3.2.5 Chat

Anders als in Diskussionsforen wird im Chat synchron kommuniziert, d. h. die Teilnehmer reagieren direkt und nicht zeitversetzt auf die Beiträge anderer. Ein Chat-Angebot kann sich eignen, um Bürgerinnen und Bürgern die direkte Online-Diskussion mit politisch Verantwortlichen oder Behördenleitungen zu ermöglichen. Dies kann zu bestimmten Anlässen oder auch regelmäßig in Form von „Online-Sprechstunden“ geschehen. Solche Chat-Angebote bedürfen noch intensiverer Werbung als Foren, da sich Adressaten in ausreichender Zahl zu einem bestimmten Zeitpunkt zusammenfinden müssen.

Abschnitt 3.2.5 Aufwand 4, Bedeutung 2

Aussagen im Chat besitzen in der Regel eine geringe Verbindlichkeit. Anders als etwa in Foren kann ein Sachverhalt im Zuge synchroner Kommunikation nicht so sorgfältig geprüft werden, wie es für eine sachgerechte Stellungnahme der Verwaltung erforderlich wäre. Häufig ist der verwaltungsseitige Chat-Partner für die angesprochenen Themen fachlich auch gar nicht zuständig oder müsste vorbindenden Aussagen Rücksprache mit anderen halten.

Geringe Verbindlichkeit

3.3 Transaktionsangebote

Die Hoffnungen, mit dem Internet Servicequalität und Wirtschaftlichkeit der Verwaltungsarbeit gleichermaßen verbessern zu können, beruhen im Wesentlichen auf den Möglichkeiten, komplette Geschäftsvorgänge zwischen Bürgern und Verwaltung übers Internet abzuwickeln. Auf diese Weise könnten der Gang zur Verwaltung oder das Zuschicken von Unterlagen per Post in vielen Fällen voll-

ständig entfallen – vorausgesetzt, die Bürger verfügen über die erforderliche Hard- und Software-Ausstattung.

Behördenseitig lassen sich durch Transaktionsangebote Einsparpotenziale durch Effizienzsteigerungen und Automatisierung (Back-Office der Behörden) sowie Standardisierung der Geschäftsprozesse erreichen. Voraussetzung für das Erzielen von Einsparpotenzialen ist dabei eine interne Geschäftsprozessanalyse und -optimierung (s. Phase 3 des Phasenplans im E-Government-Handbuch).

Für die Einführung umfangreicher Transaktionsangebote ist zunächst mit erheblichen organisatorischen und finanziellen Aufwänden zu rechnen. Bislang existieren selbst unter den Modellprojekten der Initiative BundOnline 2005 nur wenige Verfahren, die einen medienbruchfreien (d. h. vollständig elektronischen) Ablauf vom Bürger zur Behörde und zurück sicherstellen. Mit dem Hintergrund der vorab erwähnten Einsparpotenziale ist in diesem Bereich in den nächsten Jahren ein stetiger Fortschritt zu erwarten.

Anders als bei einer Informationsrecherche oder der Kontaktaufnahme via E-Mail sind für sichere und rechtsverbindliche Online-Transaktionen vielfach Komponenten erforderlich, die (noch) nicht zur geläufigen Grundausstattung privat eingesetzter PCs gehören. Manchmal sind beispielsweise Plug-Ins oder andere Zusatzprogramme erforderlich, um komplexere Transaktionen abwickeln zu können. In der Regel hat der Gesetzgeber für Bürger-Antragsverfahren die Verwendung qualifizierter elektronischer Signaturen vorgesehen, für deren Einsatz grundsätzlich Signaturkarte und Kartenlesegerät erforderlich sind. Insofern wurde die Messlatte für die Teilnahme an elektronischen Verfahren zu Gunsten einer allseitigen Rechtssicherheit und Verbindlichkeit verhältnismäßig hoch gelegt. Der Einsatz von elektronischen Signaturen ist deshalb ein Qualitätskriterium im E-Government.

Exkurs: Elektronische Signaturen

Sollen Dokumente rechtskonform übertragen werden, ist es notwendig, die entsprechenden Dokumente elektronisch zu signieren. Durch die elektronische Signatur wird zum einen manipulationssicher dokumentiert, wer der Autor einer Nachricht ist. Zum anderen kann durch Prüfung der Signatur sichergestellt werden, dass das signierte Dokument nicht nachträglich manipuliert worden ist. Rechtlich wird zwischen einfachen, fortgeschrittenen und qualifizierten Signaturen differenziert¹⁷.

Einfache elektronische Signaturen sind bereits Daten in elektronischer Form, die der Authentisierung dienen; dies können auch Namenskürzel oder eingescannte Unterschriften sein. Fortgeschrittene elektronische Signaturen müssen darüber hinaus

- ausschließlich dem Inhaber des Signaturschlüssels zugeordnet sein,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,

¹⁷ Der Einsatz elektronischer Signaturen wird durch das seit 22. Mai 2001 in Kraft getretene neue Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) geregelt.

- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich beziehen, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Qualifizierte elektronische Signaturen werden gegenüber fortgeschrittenen Signaturen zudem noch mit einem zertifizierten Kartenleser erzeugt und beruhen auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat, das seinerseits nur für natürliche Personen und von so genannten Trust-Centern ausgestellt wird.

Sofern die qualifizierte Signatur bzw. das entsprechende Zertifikat von akkreditierten Trust-Centern ausgestellt wird, kann zusätzlich noch von akkreditierten elektronischen Signaturen gesprochen werden. Die akkreditierte Signatur ist charakterisiert durch

- die Garantie einer 30-jährigen Überprüfbarkeit,
- die umfassende Evaluation aller gesetzlich geforderten technischen Produkte nach dem Stand von Wissenschaft und Technik,
- die staatliche Überprüfung der Zertifizierungsanbieter vor Aufnahme der Tätigkeit.

Dem Bürger, der mit der Verwaltung online kommunizieren möchte, sollten folglich Informationen darüber gegeben werden, welche der genannten elektronischen Signaturen durch die Internet-Plattform der Gemeinde unterstützt werden und wo er solche Signaturen erhalten kann. Wann welche Signaturqualität erforderlich ist, wird für den Bereich des Zivilrechts und des Prozessrechts im Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Formvorschriften an den modernen Rechtsgeschäftsverkehr geregelt. Für den Bereich des Verwaltungsrechts ist die Signaturqualität Gegenstand der Änderungsgesetze zum Verwaltungsverfahrensgesetz (VwVfG), zur Abgabenordnung (AO) und zum Sozialgesetzbuch (SGB). Qualifizierte Signaturen müssen demnach nur dort zum Einsatz kommen, wo bislang Schriftformerfordernis vorlag. Entsprechend dieser Vorgabe sollte der Bürger von der Verwaltung nur zur Nutzung solcher elektronischer Signaturen aufgefordert werden, die für den jeweiligen Einsatzzweck erforderlich sind.

Darüber hinaus sollte die Möglichkeit bestehen, den Zeitpunkt der Signaturerstellung durch entsprechende Zeitstempel zweifelsfrei zu dokumentieren. Das Signaturgesetz schreibt zwar nicht vor, dass der Zeitpunkt der Signaturerstellung aus der Signatur ersichtlich sein muss. Eine Signatur ist auch ohne Zeitstempel rechtskonform. Eine sichere Bestimmung des Zeitpunkts ist allerdings nur dann möglich, wenn qualifizierte Zeitstempel im Sinne des Signaturgesetzes verwendet werden.

Die eindeutige Zuordnung eines Dokuments zu dessen Autor setzt beim Empfänger der Nachricht entsprechende Prüfmechanismen voraus. So sollte sich der

¹⁸ „Weiterführende Informationen zu diesem Thema finden Sie in den Modulen „Kryptographie im E-Government“ (dort Ziff. 8) und „Authentisierung im E-Government“ (beide Module sind Teile des thematischen Schwerpunktes IV B IT und IT-Sicherheit).“

Bürger durch Prüfung von Signatur und Zertifikat von der Authentizität des Dokuments ebenso überzeugen können wie von der Gültigkeit und Authentizität des Behörden-Zertifikats selbst.

Die Signatur- und Zertifikatsprüfung ist jedoch für den Bürger, aber auch für die Verwaltung nicht gerade trivial. Es ist daher sehr hilfreich, wenn solche Prüfaufgaben an eine zentrale neutrale Stelle mit Notariatsfunktion – einen so genannten Intermediär – delegiert werden können. Die Ergebnisse aller vom Intermediär vorgenommenen Prüfungen werden in einem Prüfprotokoll vermerkt. Der Bürger bzw. die Verwaltung entscheiden dann anhand der Prüfergebnisse eigenverantwortlich, wie sie mit den übertragenen Dokumenten umgehen wollen. Protokollier- und Quittierfunktionen sind ohnehin bei einer neutralen Stelle gut aufgehoben, wenn es beispielsweise darum geht, in Streitfällen die Zustellung eines Dokuments tatsächlich nachweisen zu können.

Ein Zertifikat wird nur solchen Personen ausgestellt, die ihre Identität durch Vorlage eines Personalausweises belegen können. Aus dem sorgsamem Prozess der Zertifikatsausstellung kann jedoch nicht geschlossen werden, dass Zertifikate eine Art elektronischer Personalausweis bilden, mit dem sich der Inhaber auch in offenen Systemen ohne Medienbruch zweifelsfrei identifizieren kann. Qualifizierte Zertifikate nach dem Signaturgesetz enthalten neben Informationen über das Zertifikat (Zertifikats-Nr., Gültigkeitszeitraum) mindestens den Vornamen und den Nachnamen des Antragstellers oder ein als solches gekennzeichnetes Pseudonym. Mehr Bezugsdaten werden nur auf ausdrücklichen Wunsch und auf Kosten des Inhabers aufgenommen, soweit die Certificate-Authority (CA) dies nicht verweigert. Mit diesen Merkmalen lässt sich jedoch keine Person eindeutig identifizieren. Es besteht daher das Risiko, dass Personen die Identität eines Namensvetters vortäuschen und sich auf diese Weise missbräuchlich Zugang zu Fachverfahren erschleichen. Zwar lassen sich solche Identitätstäuschungen nachträglich nachweisen, da Vor- und Nachname mit einem eindeutigen Zertifikat signiert werden. Dies hat jedoch nur noch Auswirkungen auf mögliche Schadensersatzansprüche; der missbräuchliche Zugriff bleibt zunächst unerkannt.

Um eine eindeutige Identifizierung zu ermöglichen, wäre es erforderlich, zusätzliche Attributzertifikate gemäß Signaturgesetz auszustellen, die weitere Informationen über den Zertifikatsinhaber wie beispielsweise Geburtsdatum, Geburtsort enthalten. Solche Attribute sind jedoch zur Zeit nicht auf der Signaturkarte vorhanden, sodass diese – sofern sie nicht aufgrund früherer Authentisierungsvorgänge bereits beim Empfänger gespeichert sind – beim zuständigen Trust-Center abgerufen werden müssten. Vorab müsste der Bürger bzw. Anwender die Attributzertifikate jedoch beim Trust-Center beantragen. Eine flächendeckende Nutzung von Attributzertifikaten, die beim Zertifikatherausgeber gespeichert und zum Abruf bereit gehalten werden, existiert zurzeit jedoch nicht.¹⁸

Die Vorteile elektronischer Transaktionen beschränken sich aber nicht auf das Ersparen von Weg- und Wartezeiten oder von Portokosten. Strukturierte Dialoge können den Bürger durch eine Anwendung führen und ihm das Ausfüllen komplizierter Formulare erheblich vereinfachen. In manchen Fällen werden elektronisch

**Strukturierte
Dialoge**

veranlasste Vorgänge auch schneller bearbeitet. Dies wird den Bürgern beispielsweise bei der elektronischen Steuererklärung¹⁹ in Aussicht gestellt.

Als „Transaktionsdienste“ werden im Folgenden alle Angebote verstanden, die dazu dienen, über reine Informationen hinaus Geschäftsvorfälle zwischen Bürgern und Verwaltung durch Online-Angebote in Teilen zu unterstützen (z. B. durch das Herunterladen und Ausdrucken eines Vordrucks) oder vollständig elektronisch abzuwickeln, indem die eingegebenen Daten direkt an das Verwaltungssystem übermittelt und dort weiter bearbeitet werden.

3.3.1 Umfang und Tiefe

In welchem Umfang eine Verwaltung Transaktionsdienste anbietet und welche Tiefe dieses Angebot erreicht, d. h. in welchem Maße eine vollständige Online-Abwicklung möglich ist, hängt stark von der Aufgabenstellung, dem Stellenwert von Formularen und den Rechtsgrundlagen, die den jeweiligen Vorgängen zu Grunde liegen, ab. Um Mehrfachaufwand, z. B. bei der Erfassung von Daten, zu vermeiden, ist es sicherlich wünschenswert, wenn möglichst viele Transaktionen vollständig online durchgeführt werden könnten. In vielen Fällen müssen die dazu erforderlichen Anwendungen sowie die Schnittstellen zu den Fachverfahren aber erst noch entwickelt werden, was sich von Fall zu Fall sehr aufwändig und damit langwierig gestalten kann. Daher können Anwendungen, die Transaktionen mit der Verwaltung nur in Teilen unterstützen, durchaus sinnvoll sein, obwohl sie nicht alle Vorteile der vollständigen elektronischen Übermittlung bieten. Das Spektrum denkbarer Transaktionsangebote lässt sich u. a. danach systematisieren, wie die Bürger ihre Daten eingeben, welche Form der Übermittlung gewählt werden kann und wie die nachfolgende Kommunikation von der Verwaltung hin zum Bürger erfolgt.

**Abschnitt 3.3.1
Aufwand 4, Bedeutung 2
(langfristig 4)**

Die Dateneingabe durch die Bürger kann insbesondere auf drei Arten erfolgen:

**Dateneingabe
durch die Bürger**

- Ein Formular wird geladen, ausgedruckt und auf herkömmliche Weise ausgefüllt.
- Ein Formular wird am Bildschirm ausgefüllt.
- Dem Bürger wird nicht eine Eingabemaske nach Vorbild des Papierformulars, sondern ein speziell gestaltetes Online-Formular angeboten. Nach Eingabe aller Daten können diese gegebenenfalls nach dem Vorbild des ansonsten üblichen Papierformulars dargestellt werden.

Ob die in der „Papierwelt“ benutzten Formulare dem Bürger auch dann am Bildschirm angezeigt werden sollen, wenn die eingegebenen Daten online übermittelt werden, sollte von Fall zu Fall entschieden werden. Für eine solche Vorgehensweise spricht ein möglicher Wiedererkennungswert bei den Bürgerinnen und Bürgern, sodass beim Ausfüllen keine Umgewöhnung erforderlich wird und das neue Verfahren ebenso „amtlich“ wirkt wie der altbekannte Weg. Dagegen sprechen die hinlänglich bekannten Mängel vieler Papierformulare (unübersichtlicher Aufbau, bürokratische Formulierungen usw.) und die Unterschiede zwischen dem Ausfüll-

¹⁹ <http://www.elster.de>

len eines Papierformulars und der Dateneingabe am Bildschirm (Überblick über das komplette Formular, Navigation zwischen Formularfeldern usw.). Grundsätzlich lässt sich sagen, dass die Handhabung von originalgetreu dargestellten Formularen mit zunehmendem Seitenumfang für den Bürger immer schwieriger wird. Kommt die Entwicklung eines speziell gestalteten Online-Formulars nicht in Betracht, sollten die Eingabeseiten auf thematisch sinnvoll unterteilte, einzeln ansteuerbare Einheiten aufgeteilt werden.

Die Übermittlung des Formulars bzw. der darin enthaltenen Daten kann dann auf herkömmlichem Weg per Post, als Fax oder bei einem persönlichen Besuch oder aber auf elektronischem Weg erfolgen.

Nach dem elektronischen Versand von Daten durch den Bürger kann unterschiedlich gestalteter Service angeboten werden:

- In jedem Fall erscheint es sinnvoll, die erfolgreiche Übermittlung der Daten zu bestätigen und bei dieser Gelegenheit wenn möglich einige Hinweise zur weiteren Bearbeitung zu geben.
- Einen Schritt weiter gehen Anwendungen, mit denen der Bearbeitungsstand online abgefragt werden kann („track and trace“). Um dies zu realisieren, müssten die an einem Vorgang beteiligten Bearbeiter den jeweils aktuellen Status in einer Datenbank speichern, auf die der Bürger übers Internet zugreifen kann. Noch komfortabler wäre es, wenn die vom Bürger übersandten Daten ohne Medienbrüche in einem Workflow-System weiterbearbeitet werden, das die Stati automatisch für Abfragen übers Netz protokolliert. Es bietet sich an, nach der ersten Datenübertragung durch den Bürger diesem einen Zugangscod zurück zu übermitteln, um seine späteren Anfragen zuverlässig dem jeweiligen Vorgang zuordnen zu können.
- Ein weiterer Zusatznutzen der elektronischen Bearbeitung könnte darin bestehen, dass die Verwaltung den Bürger auf elektronischem Weg über wichtige, seinen Fall betreffende Informationen, z. B. ablaufende Fristen zur Einreichung von Dokumenten, versorgt. Auch der Stand der Bearbeitung ließe sich auf diese Weise pro-aktiv an die vom Bürger angegebenen Kontaktdaten (E-Mail, SMS) übermitteln.
- An passender Stelle sollte dem Bürger ein Kontakthinweis angeboten werden, falls sich nach Absenden der Formulare und auch noch nach Abschluss des kompletten Vorgangs, etwa nach Zustellung eines Bescheids, Klärungsbedarf ergeben sollte.

Welche der beschriebenen Varianten letztlich für welche Geschäftsvorfälle realisiert werden, hängt von einer Vielzahl von Faktoren ab.²⁰ Auf die technischen Voraussetzungen innerhalb der Verwaltung wurde zu Beginn dieses Abschnitts bereits hingewiesen. Weiterhin legen es die naturgemäß begrenzten Ressourcen nahe, mit einfachen, zügig zu realisierenden Angeboten zu beginnen und aufbauend auf den dabei gesammelten Erfahrungen komplexere Anwendungen zu entwi-

²⁰ Vgl. dazu auch die Ausführungen zur Überprüfung von Aufwand und Nutzen im Modul „Phase 3 – Analyse“, Aktivität 3.8 sowie die Bewertungskriterien des Umsetzungsnutzens einer Dienstleistung in „Bewertungskriterien für potenziell online-fähige Dienstleistungen“, Kapitel 2.

ckeln bzw. entwickeln zu lassen. Bei der Prioritätensetzung wird sicherlich auch die Frage zu beachten sein, wie oft ein Vorfall insgesamt in Anspruch genommen wird (danach bemisst sich die mögliche Entlastung für die Verwaltung) und wie häufig der einzelne Bürger mit dem betreffenden Geschäftsvorfall konfrontiert ist (danach bemisst sich der Nutzen eines Angebots für die Bürgerinnen und Bürger). Von entscheidender Bedeutung sind weiterhin die rechtlichen Voraussetzungen²¹, etwa zur Zulässigkeit einer elektronischen Signatur an Stelle der handschriftlichen Unterschrift. Zudem kann, wie bereits erwähnt, in vielen Fällen noch nicht davon ausgegangen werden, dass die Bürger über das zur Durchführung komplexer Transaktionen erforderliche Equipment (Signaturkarte, Kartenleser u.ä.) verfügen. Aus diesem Grund sollten insbesondere für Geschäftsvorfälle mit hohen Fallzahlen durchaus mehrere Transaktionsvarianten (Formular-Download, Hybridlösung, Online-Formular) angeboten werden, um möglichst vielen Bürgern einen Vorteil zu bieten.

3.3.2 Payment

Die Abwicklung von Bezahlvorgängen übers Internet ist auch für Verwaltungen ein Thema: Bei manchen Geschäftsvorfällen, die online abgewickelt werden (sollen), fallen Gebühren an, vielleicht wird auch für den Bezug bestimmter Informationen (umfangreiche Broschüren oder Dokumentationen, Kartenmaterial, Gutachten u. ä.) ein Entgelt verlangt. Die einfachste Variante wäre, dass der Bürger nach einer Online-Transaktion oder -Bestellung gebeten wird, den entsprechenden Betrag zu überweisen und nach Zahlungseingang die Weiterbearbeitung durch die Verwaltung erfolgt. Abgesehen davon, dass viele Bürger aus dem elektronischen Handel eine andere Servicequalität gewohnt sind, bringt ein solches Verfahren auch für die Verwaltung Aufwand und Nachteile mit sich. Beispielsweise wird der überwiesene Betrag einem online eingegangenen Datensatz zugeordnet werden müssen, aus dem hervorgeht, wofür das Geld verwendet werden soll und wer die betreffende Leistung wünscht.

**Abschnitt 3.3.2
Aufwand 4, Bedeutung 2**

Online-Bezahlverfahren erfordern gleich in zweifacher Hinsicht komplexe Integrationsleistungen: Zum einen muss die Bezahlung mit dem eigentlichen Geschäftsvorfall integriert werden. Bei der Bestellung einer Broschüre ist dies über ein kostengünstig erhältliches Shop-System vermutlich kein Problem. Bei Online-Transaktionen, wo sich womöglich die Höhe der Gebühr sogar erst aus den eingegebenen Daten ermitteln lässt, sind spezielle Lösungen erforderlich. Zum anderen muss das Online-Bezahlverfahren in das bestehende Kassenverfahren integriert werden, damit die so eingenommenen Gelder korrekt verbucht werden können. Beispielsweise muss online ein Kassenzichen vergeben werden können.

Komplexe Integrationsleistungen

Insgesamt kommen vier Bezahlverfahren in Betracht, die auch außerhalb des Internets praktiziert werden:

- die Online-Überweisung von einem Konto auf ein Konto der betreffenden Behörde,

²¹ Vgl. dazu auch die Ausführungen zur Vorabprüfung rechtlicher Rahmenbedingungen im Modul „Phase 3 – Analyse“, Aktivität 3.7

- die Lastschriftinzugsermächtigung,
- die Zahlung mit Kreditkarte sowie
- bei entsprechender Ausstattung mit einem Kartenleser die Zahlung mittels Geldkarte.

So genannte Micropayment-Verfahren und -Systeme, die nur innerhalb des Internets angeboten werden, bringen für den Anbieter ein gewisses Maß an Unsicherheit mit sich. Die Anbieter dieser Verfahren haben oft keine Verankerung in der Kreditwirtschaft. Viele von ihnen haben den Betrieb schon nach kurzer Zeit aufgrund zu geringer Teilnehmerzahlen wieder einstellen müssen. Ähnliches gilt für Verfahren, mit denen die Bezahlung übers Mobiltelefon erfolgen kann.

Micropayment

Die im Internet weit verbreitete Bezahlung per Kreditkarte stößt in der öffentlichen Verwaltung noch immer auf Vorbehalte, da Provisionszahlungen an die Kreditkartenorganisation erfolgen müssen. Diese Gebühren sind bei der Geldkarte deutlich niedriger. Noch sind allerdings die für den Online-Einsatz der Geldkarte zugelassenen Kartenleser mit Display und numerischer Tastatur recht teuer und dementsprechend wenig verbreitet.

Kreditkarte und Geldkarte

Wo bisher schon Rechnungen und Bescheide verwendet und Überweisungen erwartet wurden, kann an dieser Praxis auch bei der Online-Abrechnung festgehalten werden. Mahnungen können vermieden werden, wenn statt dessen eine Einzugsermächtigung verlangt wird. Diese kann in den Verwaltungsvorgang so eingebunden werden, dass er ohne solche Ermächtigung nicht zu Ende geführt werden kann.

Überweisung

Lastschriftinzugsermächtigungen im Einzelhandel werden in der Regel unterschrieben. Kommt hier online keine elektronische Signatur zum Einsatz, fehlt eine solche Unterschrift bei Online-Transaktionen. Es ist dann nicht auszuschließen, dass ein Bürger nachträglich der Abbuchung erfolgreich widerspricht. Dieses Risiko ist erfahrungsgemäß jedoch äußerst gering. Die Summe der dadurch entgangenen Einnahmen dürfte deutlich unter den Kosten der anderen Verfahren liegen.

Lastschriftinzugsermächtigung

Auch beim Payment gilt, dass die nutzerseitig erforderlichen Angaben auf formale Korrektheit und Stimmigkeit geprüft werden sollten und die Eingaben so komfortabel wie möglich gestaltet werden sollten. Beträge sollten aus Transaktionsanwendungen an das Bezahlmodul übergeben werden, Eingaben zu Kontonummer, Bankleitzahl oder Kreditkartennummer sollten nur gemäß der geltenden Konventionen akzeptiert werden. Eine lokal auf dem Webserver hinterlegte Liste der Bankleitzahlen (diese muss aber kontinuierlich gepflegt werden) kann die Eingabe (und die Überprüfung der Eingabe) der Bankverbindung zusätzlich erleichtern.

Da nicht davon ausgegangen werden kann, dass alle Bürger bezüglich der Zahlung übers Internet die gleichen Präferenzen verfolgen, über die zum Teil erforderliche Infrastruktur verfügen oder bei Micropayment-Anbietern registriert sind, sollten stets mehrere Bezahlvarianten parallel angeboten werden. Für den Bereich der Bundesverwaltung wird derzeit eine Basiskomponente „Zahlungsverkehrsplattform“ entwickelt. Eine Beschreibung der Basiskomponenten soll in Kürze im Handbuch aufgenommen werden.

3.3.3 Nutzungsqualität

3.3.3.1 Einbindung in das Gesamtangebot

Die Qualität eines Transaktionsangebots hängt ganz entscheidend von dessen Einbindung in das gesamte Web-Angebot einer Verwaltung ab.

**Abschnitt 3.3.3.1
Aufwand 3, Bedeutung 3**

Das betrifft zum einen die Auffindbarkeit: Formulare sollten über die zu den betreffenden Geschäftsvorfällen bereitgestellten Informationsseiten direkt aufrufbar sein. Weiterhin könnte eine eigene Auflistung aller bereitgestellten Formulare und Transaktionsangebote sinnvoll sein. Dies setzt aber eine sinnvolle und dem Bürgerblick folgende Verschlagwortung voraus (s. 2.2.1). Eine Liste, in der unter dem Buchstaben ‚A‘ lauter „Anträge auf...“ zu finden sind, hat nur einen sehr geringen Nutzwert. Besser wäre es, den jeweiligen Geschäftsvorfall treffend zu bezeichnen, dann das Formular zu spezifizieren und dazu auch mehrere Varianten anzubieten (also z. B. „Einkommenssteuererklärung – Anlage Kinder“ ebenso wie „Anlage Kinder zur Einkommenssteuererklärung“).

**Auffindbarkeit der
Formulare**

Zum anderen sollte an zentraler Stelle erklärt werden, wie Transaktionen online durchgeführt werden, welche Angebote diesbezüglich vorhanden sind, wie sich deren Ablauf gestaltet und mit welchen technischen Voraussetzungen unterschiedliche Transaktionsdienste im Einzelfall verbunden sind. Für Fragen zur Technik sollte ebenso eine Kontaktstelle benannt werden wie für inhaltliche Fragen zu den einzelnen Geschäftsvorfällen.

**Beschreibung des
Transaktions-
ablaufs**

3.3.3.2 Relation zum technischen Aufwand

Elektronische Signaturen ermöglichen es, auch solche Geschäftsvorfälle online zu erledigen, für die bis vor kurzem noch handschriftliche Unterschrift(en) erforderlich waren. Die damit verbundene Sicherheit und Rechtsverbindlichkeit ist allerdings mit zusätzlichem Aufwand verbunden. Dieser resultiert aus der erforderlichen Hardware-Ausstattung, den Gebühren für eine Signaturkarte, längeren Ladezeiten für aufwändige Programme usw. Nicht überall, wo heute ein Formular unterschrieben wird, ist jedoch eine Unterschrift bzw. eine elektronische Signatur erforderlich.

**Abschnitt 3.3.3.2
Aufwand 4, Bedeutung 4**

Grundsätzlich sollte dem Bürger nur der Aufwand abverlangt werden, der für zwingend erforderlich gehalten wird. Fordert der Gesetzgeber beispielsweise gar keine Unterschrift, sollte nur in begründeten Ausnahmefällen eine qualifizierte elektronische Signatur verwendet werden. Dies schließt nicht aus, dass Bürgerinnen und Bürger, die über eine Signaturkarte verfügen, diese auch für solche Vorgänge einsetzen, in denen beispielsweise auch eine fortgeschrittene Signatur oder eine ganz andere Authentisierungsvariante ausgereicht hätte²². Verwaltungen sollten also eine Technik einsetzen, die gerade bei der Authentisierung skalierbar ist, und nur dann auf Signaturen bestehen, wenn diese auch tatsächlich erforderlich sind.

**Möglichst wenig
Aufwand für die
Bürger**

²² siehe hierzu auch das Modul „Authentisierung im E-Government“

Der Aufwand aus Bürgersicht kann noch in einem weiteren Punkt vermindert werden: Meist sind es immer die gleichen Angaben, die z. B. zur Person zu machen sind. Ein komfortables Transaktionsangebot könnte daher die Möglichkeit vorsehen, lokal auf dem Client-Rechner einen geschützten Datensatz in vorgegebener Struktur anzulegen, der solche immer wieder abgefragten Daten enthält. Muss dann ein Formular ausgefüllt werden, könnte die Datei durch den Bürger geladen werden, um die darin enthaltenen Daten ins Formular einzulesen. Eine andere Option besteht darin, ähnlich wie bei Kreditinstituten oder Fluggesellschaften, einmal einen Stammdatensatz der Kunden auf einem gesicherten Server abzulegen und zukünftig Formulare, in denen die Stammdaten bereits eingetragen sind, von dort aus aufzurufen. Dies erfordert zwingend die Einwilligung des Nutzers, die jederzeit widerrufbar sein muss (s. dazu auch 5.2.3). Beide Varianten – sowohl die Speicherung der Stammdaten auf dem Client-Rechner als auch die Hinterlegung auf einem Server – setzen technisch fortgeschrittene Transaktionslösungen voraus.

**Stammdaten
hinterlegen**

3.3.3.3 Medienbruchfreiheit

Bei vielen Verwaltungsvorgängen sind Anlagen erforderlich. Soll trotzdem die elektronische Übermittlung der vom Bürger eingegebenen Daten angeboten werden, kann dieser Anforderung wiederum auf zweierlei Weise entsprochen werden:

**Anlagen auf Pa-
pier**

Anlagen können zum einen als Datei oder als eingescannte Grafik einem Online-Antrag beigelegt werden, zum anderen ist eine hybride Variante denkbar, bei der die Daten zwar elektronisch, die dazugehörigen Unterlagen aber per Post übermittelt werden. Diese zweite Variante sollte so konzipiert werden, dass die Zuordnung elektronisch eingegangener Daten zum Posteingang möglichst einfach möglich ist. Denkbar wäre z. B. die Vergabe einer Kennziffer, die der Postsendung beizufügen ist und über die der betreffende Datensatz aufgerufen werden kann. Alternativ könnte auch der Aufdruck eines Barcodes infrage kommen. Als weiterer Service könnte auch ein Anschriftenblatt zur Verwendung in Fensterbriefumschlägen zum Ausdruck angeboten werden, sodass der Bürger seine Unterlagen nur noch eintüten und frankieren muss.

**Abschnitt 3.3.3.3
Aufwand 4, Be-
deutung 4**

Diese Hybridvariante kann auch bei manchen Vorfällen Anwendung finden, bei denen eine elektronische Signatur erforderlich wäre. Bürger, die nicht über eine Signaturkarte verfügen, könnten einen Vorgang ebenfalls vollständig elektronisch übermitteln, sich abschließend eine Zusammenfassung der Daten ausdrucken, diese unterschreiben und an die Behörde senden. Solange Signaturkarten kaum verbreitet sind, könnten solche Hybridformen durchaus Zuspruch finden. Voraussetzung ist allerdings, dass nicht nur die Verwaltung davon profitiert, indem sie sich den Erfassungsaufwand ersparen kann, sondern auch den Bürgern ein Vorteil geboten wird. Dieser könnte in der Unterstützung bei der Dateneingabe durch einen strukturierten Dialog oder in der schnelleren Bearbeitung seitens der Verwaltung bestehen.

Von einem vollständig online abgewickelten Vorgang kann eigentlich erst dann die Rede sein, wenn auch das Ergebnis der verwaltungsseitigen Bearbeitung, in der Regel also ein Bescheid, online übermittelt werden kann. Solche Bescheide

**Signierte Be-
scheide der Ver-
waltung**

werden in der Regel mittels qualifizierter elektronischer Signatur zu signieren sein, sodass der Bürger ein gerichtsfestes elektronisches Dokument erhält.

3.3.3.4 Plattformunabhängigkeit

Auch für Transaktionsangebote gilt, dass diese zu möglichst vielen nutzerseitig eingesetzten Konfigurationen kompatibel sein sollten (s. 1.1.2). Dies betrifft den reinen Formular-Download ebenso wie komplexere Transaktionsdienste.

Aufwand speziell,
Bedeutung 4

Download-Formulare sollten durchgängig in einem gebräuchlichen Format angeboten werden, das von unterschiedlichen Plattformen „verstanden“ wird und weitgehend sicherstellt, dass es beim Ausdruck nicht zu relevanten Veränderungen gegenüber der von der Verwaltung vorgegebenen Gestaltung kommt bzw. kommen kann. Ein solches, derzeit weit verbreitetes Format ist das auf der Druckersprache Postscript basierende Portable Document Format (PDF). Bei der Erstellung einer PDF-Datei erfolgt quasi eine Druckausgabe in Dateiform, durch die es möglich wird, neben dem Inhalt auch das Layout eines Dokuments zu übermitteln. Die zur Betrachtung von PDF-Dokumenten erforderliche Software ist kostenlos verfügbar und inzwischen weit verbreitet. Sie lässt sich aus dem Browser heraus aufrufen. Um Verfälschungen am Formulartext zu vermeiden, sollten PDF-Dokumente schreibgeschützt werden. (Nachteilig ist dann allerdings, dass schreibgeschützte PDF-Dokumente nicht mehr von unterstützenden Tools im Sinne der Barrierefreiheit genutzt werden können.) Bei der Auswahl solcher plattformunabhängigen Formate sollte sich eine Verwaltung an den Empfehlungen von SAGA²³ orientieren. Proprietäre Formate, etwa aus dem Office-Bereich, sollten allenfalls zusätzlich zu einem solchen Format bereitgestellt werden.

Anbieter unter-
schiedlicher Da-
tenformate

Komplexere Transaktionen werden häufig in der plattformunabhängigen Programmiersprache Java realisiert. Java wird zwar nicht von allen Browsertypen standardmäßig unterstützt, die benötigten Software-Module sind aber gegebenenfalls ohne Zusatzkosten im Internet zu erhalten.

Java

3.3.3.5 Handhabung von Formularen

Im Unterschied zu Vordrucken auf Papier bestehen bei Formularen, die am Bildschirm ausgefüllt werden, vielfältige Möglichkeiten, den Bürger bei dieser Tätigkeit durch Hinweise, Plausibilitätsprüfungen usw. zu unterstützen, ihm so die Eingaben zu erleichtern und fehlerhafte Angaben zu vermeiden. In gewissem Ausmaß kann derartige Unterstützung auch schon angeboten werden, wenn die Originalvordrucke weiterverwendet werden. Weitergehende Hilfen lassen sich insbesondere bei eigens programmierten Eingabemasken und -dialogen realisieren.

Abschnitt 3.3.3.5
Aufwand 2, Be-
deutung 3

Ausfüllhilfen: Erläuternde Hinweise können zu Beginn des Formulars angeboten werden. Hilfreicher wird es aber sein, wenn zu einzelnen Eingabefeldern erklärt wird, welche Angaben in welcher Form und gegebenenfalls auch aus welchem

²³ S. Fußnote 2

Grund an dieser Stelle benötigt werden. Technisch lässt sich dies auf ganz unterschiedliche Weise realisieren: Die Erläuterungen können z. B. in einem dafür vorgesehenen Bereich oder in einem neu geöffneten Fenster erscheinen, sobald der Cursor in das betreffende Eingabefeld gesetzt wurde. Weniger umfangreiche Erklärungen können auch als „Mouse over“ realisiert werden und erscheinen, wenn der Mauszeiger über das Feld gezogen wird.

Verdeckte Felder: Manche Angaben werden nicht generell, sondern nur in bestimmten Fällen benötigt. Frauen müssen keine Angaben zum Wehrdienst machen, Männer nicht nach Schwangerschaften gefragt werden. Online-Formulare können so programmiert werden, dass derartige Felder zwar mitgeladen werden, aber nur dann eine Eingabe verlangt wird, wenn die zuvor abzufragenden Voraussetzungen für ihre Relevanz auch erfüllt sind. Komplexere Formulare lassen sich so gestalten, dass an passender Stelle (meist zu Beginn) einige Fragen zu beantworten sind und anschließend nur die relevanten Formulareile angezeigt werden. Dies beschleunigt das Ausfüllen und vermeidet Irritationen.

Automatische Vervollständigungen: Ebenso ist es möglich, Felder in Abhängigkeit von zuvor getätigten Eingaben automatisch zu vervollständigen. Wird beispielsweise nach Ortsangaben gefragt, könnte in solche Felder evtl. zunächst der zuvor abgefragte Wohnort übernommen werden. Sollte diese Angabe nicht zutreffen, kann der Bürger sie einfach ändern. Trifft sie zu, übernimmt er die automatische Voreinstellung.

Defaultwerte: An manchen Stellen kann es auch hilfreich sein, Voreinstellungen (Defaultwerte) vorzugeben, die dann gegebenenfalls geändert werden müssen. Von dieser Möglichkeit sollte aber nur sparsam Gebrauch gemacht werden, um zu verhindern, dass unzutreffende Voreinstellungen aus Flüchtigkeit übernommen werden. In jedem Fall sollten diese Defaultwerte der deutlichen Mehrzahl der Fälle entsprechen. Es ist beispielsweise wenig sinnvoll, bei der Frage nach dem Geschlecht einen (wie auch immer gewählten) Defaultwert zu setzen.

Eingabeüberprüfungen: Die Eingaben im Formular sollten soweit wie möglich vor Absenden an die Behörde auf Stimmigkeit überprüft werden²⁴. Dies betrifft sowohl die Vollständigkeit als auch die Plausibilität der Angaben. Solche Prüfungen vermeiden mit vergleichsweise geringem Programmieraufwand Missverständnisse und Rückfragen im Zuge der weiteren Bearbeitung. Die angemerkten Fehler sollten dem Bürger deutlich angezeigt werden. Im Einzelfall wird sicherlich auch eine Erläuterung sinnvoll sein, warum eine Eingabe nicht akzeptiert wird. Beispielsweise könnte es ja erforderlich sein, eine fehlerhafte Angabe an früherer Stelle zu korrigieren, damit die sachlich richtige Eingabe zum späteren Zeitpunkt von der Plausibilitätsprüfung akzeptiert wird. Der bloße Hinweis auf eine „unplausible“ oder „fehlerhafte Eingabe“ allein wird den Bürgern gerade bei komplexen Formularen in vielen Fällen nicht weiterhelfen.

²⁴ Eine Prüfung der Inhalte (Plausibilität, erlaubte Zeichen und Werte in Formularfeldern, ...) ist aus Gründen der IT-Sicherheit aber unbedingt serverseitig zu wiederholen.

4 IT-Sicherheit

Die IT-Sicherheit von Web-Auftritten und E-Government-Dienstleistungen ist nicht nur Grundvoraussetzung für das ordnungsgemäße Funktionieren solcher Angebote sondern zugleich auch ein wichtiges Element für deren Akzeptanz. Bürgerseitig gibt es eine klare Erwartungshaltung an die Behörden, die Sicherheit von E-Government-Verfahren zu gewährleisten. Ein Bürger, der teils erheblichen Technikaufwand betreiben muss, um an E-Government-Dienstleistungen teilnehmen zu können, hat einen Anspruch darauf, sich nicht zusätzlichen Sicherheitsrisiken ausgesetzt zu sehen. Der Bürger hat mit der klassischen Postversendung ein aus seiner Sicht etabliertes und sicheres Verfahren, welches nur durch ein elektronisches Verfahren mit mindestens gleichwertigem Sicherheitsniveau abgelöst werden sollte.

Der Bürger muss darauf vertrauen können, dass seine schützenswerten Informationen auch in hoch komplexen IT-Verfahren an jeder Stelle des Bearbeitungsprozesses angemessen geschützt werden. Da es dem Bürger nicht möglich ist, die Verfahrenssicherheit selbst zu überprüfen, wird er nach dem Motto „die machen das für mich“ auf verlässliche und klare Aussagen der Behörden hierzu angewiesen sein. Durch die Nutzung von elektronischen Signaturen im E-Government, die es dem Bürger ermöglichen sollen, von jedem beliebigen Punkt und zu jeder beliebigen Zeit seine Anträge elektronisch abzusenden, wird die Beherrschbarkeit der IT-Sicherheit in den Verwaltungen vor neue Herausforderungen gestellt.

Abgesehen von den Gefahren, die grundsätzlich für den PC des Bürgers bestehen (z. B. durch Computerviren), ist im Bereich des E-Government sicherzustellen, dass

Sicherheitsziele

- der Web-Auftritt nicht unberechtigt manipuliert werden kann,
- sensible Inhalte zwischen Bürger-Client und Web-Server vertraulich übertragen werden können,
- Web-Server und Bürger-Client sich gegenseitig authentisieren können.

Der Aufwand für die Realisierung der genannten Sicherheitsziele steigt überdurchschnittlich mit der Klassifikations- und Komplexitätsstufe der jeweiligen E-Government-Dienstleistung (s. 3): In der Regel ist es deutlich aufwändiger, eine angemessene IT-Sicherheit für Transaktionsangebote zu erreichen als für traditionelle Informationsangebote. Bei ausschließlichen Informationsangeboten für den Bürger steht die ständige Verfügbarkeit des Web-Servers über das Internet im Vordergrund (Behördeninformationen, Formulare). Im Gegensatz hierzu sind komplexe Transaktionsverfahren zu sehen, die behördenseitig elektronisch signierte Bürgeranträge automatisiert in Workflow-Systeme der Verwaltung weiterleiten. Bei solch komplexen E-Government-Verfahren überwiegt in der Regel der Schutzbedarf hinsichtlich der Vertraulichkeit und Integrität der Daten sowie der Nichtabstreitbarkeit der Autorenschaft.

Das Bundesamt für Sicherheit in der Informationstechnik hat zur Steigerung der IT-Sicherheit – vor allem im behördlichen Bereich – bereits zahlreiche Dokumente veröffentlicht, die auch bei der Implementierung sicherer E-Government-

Dienstleistungen berücksichtigt werden sollten (die angegebenen Hilfsmittel finden Sie auch im Werkzeugkasten des E-Government-Handbuchs):

- Das IT-Grundschutzhandbuch (<http://www.bsi.bund.de/gshb>) stellt im genannten Kontext wichtige Informationen für Fachleute bereit. Durch die Nachbildung eines Schichtenmodells wird dem E-Government-Koordinator oder dem IT-Sicherheitsbeauftragten der Verwaltung die Möglichkeit eröffnet, sich zügig einen Überblick über Maßnahmen zur IT-Sicherheit zu verschaffen.
- Mit der Einführung des IT-Grundschutz-Zertifikates ist Behörden eine zusätzliche Möglichkeit gegeben worden, den erreichten Status der IT-Sicherheit als Qualitätsmerkmal zu propagieren (<http://www.bsi.bund.de/gshb/zert/allge.htm>).
- Hilfestellungen für Entscheider oder Fachverantwortliche zur Planung und Konzeption von Web-Auftritten von Verwaltungen werden im E-Government-Handbuch ausführlich im Modul „Sicherer Internetauftritt im E-Government“ (http://www.bsi.bund.de/fachthem/egov/download/4_IntAuf.pdf) erörtert.
- Wer noch weitergehende Hintergründe für die Implementierung verlässlicher Firewall-Systeme braucht, erhält diese in der vom BSI veröffentlichten „Firewall-Studie 2001“ (<http://www.bsi.bund.de/literat/studien/firewall/fwstud.htm>).
- Maßnahmen zum Einsatz von kryptographischen Verfahren zum sicheren Verbindungsaufbau, zur gegenseitigen Authentisierung der Kommunikationspartner sowie zur sicheren Informationsübertragung sind in anderen Modulen des E-Government-Handbuchs veröffentlicht.
- Informationen zu Standards und Architekturen für das E-Government erhält man unter <http://www.bund.de/SAGA>.

BSI-Quellen

Aufgrund dieser schon zahlreich vorliegenden Dokumente werden die Inhalte in diesem Abschnitt nicht mehr ausführlich aufgearbeitet. Es wird vielmehr darauf eingegangen, welche Themen von den jeweils Verantwortlichen berücksichtigt werden sollten, wenn es darum geht, eine insgesamt sichere E-Government-Dienstleistung anzubieten, und warum dies die Qualität des Web-Auftritts nachhaltig steigert.

4.1 IT-Sicherheitsmanagement

IT-Sicherheit sollte von den Behörden als wesentlicher Bestandteil jeder E-Government-Dienstleistung verstanden, folglich ein IT-Sicherheitsmanagement als dauerhafte Aufgabe innerhalb der Verwaltungsstruktur verankert werden. Mit der beabsichtigten Verschiebung der Aufgabenbewältigung hin zu einer vollständig elektronischen Abwicklung der Geschäftsvorfälle steigt die Bedeutung eines planvollen IT-Sicherheitsmanagements deutlich. Eine ausführliche Beschreibung, welche Maßnahmen veranlasst werden können, ist im IT-Grundschutzhandbuch unter <http://www.bsi.bund.de/gshb/deutsch/b/30.htm> zu finden. Im Kontext des E-Government-Handbuchs bietet es sich an, einem kompetenten Mitarbeiter die

Abschnitt 4.1
Aufwand 3, Bedeutung 3

Funktion eines behördlichen IT-Sicherheitsbeauftragten zu übertragen, der insbesondere folgende Aufgaben wahrnimmt:

- Sorgfältige Auswahl von externen Internet-Dienstleistern,
- Erstellung und Fortschreibung eines IT-Sicherheitskonzepts der Behörde,
- Verantwortung für die regelmäßige Prüfung der Web- und Mail-Server-Integrität, beispielsweise durch Auswertung von Log-Files,
- Analyse des Antwort-Zeitverhaltens des Web- und Mail-Servers, insbesondere notwendig bei ständig steigender Zahl von Zugriffen,
- Veranlassung der Prüfung der zum Download bereitstehenden und per E-Mail oder CD versendeten Inhalte auf Virenfreiheit und Schadfunktionen.

**Aufgaben eines
IT-Sicherheits-
beauftragten**

4.2 Erklärungen der Behörde zur IT-Sicherheit

Entweder gemeinsam mit der Datenschutzerklärung oder als separate Informationsseite sollte der Web-Auftritt zusätzlich eine Selbsterklärung der Behörde zu sicherheitstechnischen Fragen des Angebotes bereithalten. Transaktionsangebote im Internet sind in der Vorstellung vieler Bürger noch immer mit dem – vermeintlichen – Makel der Unsicherheit behaftet. Dem kann mit einer leicht verständlichen Erklärung zu sicherheitstechnischen Fragen aktiv begegnet werden. Auch und gerade in diesem Bereich kann durch größtmögliche Transparenz das notwendige Vertrauen des Bürgers in die Vorteilhaftigkeit der Nutzung des Online-Angebots geschaffen werden. Dem Bürger sollten daher folgende Sicherheitsinformationen zum Web-Auftritt der Behörde mitgeteilt werden, soweit diese nicht als vertraulich einzustufen sind (siehe 7. Mustertexte):

**Abschnitt 4.2
Aufwand 1, Be-
deutung 3**

- Hinweise auf technische Ansprechpartner mit E-Mail-Adresse, an die sich die Bürger bei Fragen zur Sicherheit wenden können (s. 4.1).
- Informationen darüber, durch welche Vorkehrungen sich der Bürger selbst schützen kann (Browser-Einstellungen, Personal Firewall etc., s. 4.3)
- Informationen darüber, welche Vorgänge, Transaktionen und E-Mail-Kommunikation verschlüsselt werden (können), welche Schlüssellänge eingesetzt wird und welchen Sicherheitsrisiken damit begegnet wird (s. 4.4),
- Informationen zu Sicherheitstechniken auf dem Web-Server und der Einsatzumgebung (s. 4.5), ggf. Hinweise auf Zertifikate und Gütesiegel, die im Rahmen eines Datenschutzaudits oder nach einer Revision der IT-Sicherheit vergeben worden sind.

**zu veröffent-
lichende Sicher-
heitsinformatio-
nen**

4.3 Aktive Inhalte

Die Funktionalität eines Web-Auftritts ist im Allgemeinen auf die Möglichkeiten von HTML beschränkt. Diese Funktionalität kann auf zwei Arten erweitert werden, durch das Einbetten von Programmcode in HTML-Seiten per ActiveX, Java oder JavaScript, sofern der Browser entsprechend konfiguriert ist, oder durch Erweiterung der Browser-Funktionalität mit Hilfe von Plug-Ins. ActiveX, Java, Ja-

**Aufwand 2, Be-
deutung 3**

vaScript oder Plug-Ins werden als aktive Inhalte bezeichnet. Aktive Inhalte können insbesondere eine Gefährdung der Integrität eines PC darstellen. Durch die Ausführung entsprechender Codes auf dem Rechner können, ohne dass der Nutzer dies will oder weiß, beispielsweise Inhalte gelöscht oder manipuliert werden oder vertrauliche Informationen an Dritte übermittelt werden.

Wenn das Informationsangebot auf einer oder mehreren der genannten Technologien basiert, ist der Nutzer dieses Angebots gezwungen, die Ausführung von aktiven Inhalten auf seinem Rechner zuzulassen oder auf die Nutzung zu verzichten. Lässt der Bürger die Ausführung aktiver Inhalte zu, entstehen ihm potenzielle Risiken. Außerdem besteht die Gefahr, dass der Bürger das Ausführen aktiver Inhalte später nicht wieder einschränkt bzw. deaktiviert und somit für Angriffe über aktive Inhalte unsicherer Quellen anfällig bleibt.

Bei der Gestaltung des Informationsangebots sollte daher möglichst auf aktive Inhalte verzichtet werden. Sollen dennoch dynamische Inhalte angeboten werden, sollten diese Inhalte serverseitig (z. B. mittels PHP) erstellt werden. Dies ist bei der sicheren Administration des WWW-Servers entsprechend zu berücksichtigen. Kann auf die Verwendung aktiver Inhalte auf keinen Fall verzichtet werden, sollten die aktiven Inhalte unbedingt von einer allgemein als vertrauenswürdigen anerkannten Stelle (z. B. einem Trust-Center) signiert sein. Insgesamt sollte der Bürger möglichst umfassend über die Gefahren informiert und an die Deaktivierung erinnert werden. Das Thema „aktive Inhalte“ wird ausführlich im Modul „Sicherer Internetauftritt im E-Government“ erörtert.

möglichst Verzicht auf aktive Inhalte

4.4 Kryptografie und Verbindungssicherheit, Authentisierung²⁵

Wenn Informationen unverschlüsselt gesendet werden, können sie auf ihrem Weg zum Empfänger von Dritten unbemerkt eingesehen werden. Durch eine Verschlüsselung der Daten kann dagegen die Nutzung des Informationsangebots vertraulich erfolgen. Dies ist besonders dann von großer Bedeutung, wenn der Inhalt der Kommunikation sensible Informationen enthält.

Abschnitt 4.4 Aufwand 3, Bedeutung 4

Um eine vertrauliche Datenübertragung zu ermöglichen, muss allerdings auch die Authentizität des Kommunikationspartners mithilfe einer vertrauenswürdigen Quelle überprüfbar sein. Gelingt dies nicht, könnte sich ein potenzieller Angreifer z. B. als WWW-Server ausgeben und so trotz Verschlüsselung die Kommunikation belauschen.

Die Verschlüsselung kann von Rechner zu Rechner (WWW-Client zu WWW-Server) oder auch von Bürger zu Bürger (Bürger zu Sachbearbeiter) erfolgen. Die Absicherung der Kommunikation zwischen WWW-Client und WWW-Server (Rechner-zu-Rechner) sichert allerdings nicht den gesamten Kommunikationsweg vom Bürger zum Sachbearbeiter ab.

²⁵ Die Fragen dieses Abschnitts stellen die Verbindung zu den Maßnahmen des Abschnitts „Kryptografie im E-Government“ in Kapitel IV B „IT und IT-Sicherheit“ her.

Die Sicherheit der Kommunikation hängt dabei wesentlich von der Qualität der eingesetzten Verschlüsselungsverfahren (symmetrische und asymmetrische Verschlüsselung) und der verwendeten Schlüssellänge ab. Werden unsichere kryptographische Verfahren oder Protokolle verwendet, kann ein Angreifer die Schwachstellen dieser Schutzmechanismen ausnutzen und sie überwinden. Als Verschlüsselungsprotokolle bzw. -verfahren haben sich inzwischen SSLv3 und TLS etabliert. Für symmetrische Verfahren gilt zur Zeit eine Länge von mindestens 128 Bit, für asymmetrische Verfahren eine Schlüssellänge von mindestens 1024 Bit. Die verwendeten Zertifikate sollten möglichst von einem anerkannten Trustcenter ausgestellt worden sein sowie schnell und zuverlässig bei diesem Trustcenter überprüft werden können.

**Verschlüsselungsverfahren
SSL/TLS, RSA**

Der WWW-Server sollte folglich eine sichere Kommunikationsverbindung nur unter Verwendung sicherer Verfahren und Protokolle akzeptieren. Hinsichtlich der verwendeten Schlüssellängen sollte der WWW-Server so konfiguriert sein, dass auch längere Schlüssellängen akzeptiert werden.

4.5 Absicherung von Web-Servern per Firewall

Ohne einen besonderen Schutz kann ein Web-Server über Internet- bzw. Intranet-Verbindungen weit gehend analysiert werden. Aus den Ergebnissen dieser Analyse können Rückschlüsse auf die Konfiguration, die verfügbaren Dienste und damit auf mögliche Schwachpunkte des Web-Servers gezogen werden. Diese können als Grundlage für einen gezielten Angriff auf den Web-Server dienen, sofern solche Analysen nicht durch den Einsatz eines Firewallsystems (z. B. durch Komponenten wie Paketfilter oder Application-Gateways) erschwert oder verhindert werden.

**Abschnitt 4.5
Aufwand 2, Bedeutung 4**

Im Gegensatz zu einem Paketfilter ist ein Application-Gateway in der Lage, Datenpakete anwendungsspezifisch zu analysieren. Die anwendungsabhängige Analyse kann durch so genannte Proxy-Server erfolgen. Je intensiver die Analyse erfolgt, desto höher ist das Schutzniveau, das durch eine geeignete Konfiguration erreicht werden kann.

Application-Gateway

Die Konfiguration von Firewall-Komponenten kann daher komplex werden, wenn der Datenverkehr möglichst genau auf die erforderliche Kommunikation beschränkt werden soll. Ein Ansatz besteht darin, alle Verbindungen grundsätzlich zu erlauben und die unerwünschten Verbindungen zu verbieten (positiver Ansatz). Alternativ dazu können grundsätzlich alle Verbindungen verboten und für erforderliche Verbindungen Ausnahmen definiert werden (negativer Ansatz).

Der positive Ansatz für die Konfiguration von Firewallkomponenten ist im Allgemeinen komplexer und somit unsicherer als der negative Ansatz. Die Menge der unerwünschten Verbindungen umfassend zu definieren, ist sehr schwierig, weil sämtliche möglichen Verbindungen bedacht und sämtliche zu unterbindenden Verbindungen definiert werden müssen. Meistens ergibt sich daraus eine sehr große Regelmenge, die dementsprechend schwer zu administrieren ist. Zusätzlich birgt dieser Ansatz ein weiteres Sicherheitsrisiko: Wird eine unerlaubte Verbindung bei der Regeldefinition für den Paketfilter übersehen oder ist die Regel fehlerhaft, wird die Verbindung aufgrund des positiven Ansatzes erlaubt und somit die Sicherheit des Systems kompromittiert.

positiver Ansatz

Um den negativen Ansatz für die Konfiguration einer Firewallkomponente zu verwenden, müssen alle erwünschten Verbindungen möglichst genau spezifiziert werden. Auf diesen Spezifikationen werden die Ausnahmeregelungen für den Paketfilter entworfen. Neben einer detaillierten Übersicht über die Verbindungsarten hat dieser Ansatz den Vorteil, dass die zu verwaltende Regelmenge im Allgemeinen wesentlich kleiner ist als im positiven Ansatz. Dementsprechend ist auch die Administration dieser Regeln einfacher. Ein fehlerhafter oder unvollständiger Regelsatz verhindert zwar eine (potenziell gewünschte) Verbindung, jedoch bleibt der Schutz erhalten, da auch potenziell unerwünschte Verbindungen verhindert werden.

negativer Ansatz

Für die Konfiguration eines Application-Gateway ist es ferner notwendig, die erforderlichen Verbindungen inklusive ihrer Inhalte zu spezifizieren. Werden nicht alle Verbindungen inklusive ihrer Inhalte spezifiziert, besteht die Gefahr, dass die Konfiguration des Application-Gateway zwar auf die Verbindung, nicht jedoch auf den tatsächlichen Inhalt der Verbindung bezogen wird. Die Analyse der Inhalte durch das Application-Gateway kann auf diese Weise teilweise oder ganz wirkungslos bleiben. Insbesondere Protokolle mit der so genannten Eigenschaft „firewall-friendly“ können sich hierbei als schwierig erweisen. Hierbei werden Daten eines Protokolls (z. B. SOAP) über ein anderes Protokoll und dessen Verbindung (z. B. HTTP) gesendet, wodurch eine Analyse der Datenpakete aufgrund des erweiterten Kontextes der Verbindung erschwert oder ganz verhindert wird.

Analyse der Inhalte

4.6 Administration von Web-Servern

Eine manipulationssichere Administration des Web-Portals ist Grundvoraussetzung für ein sicheres Internetangebot von Bund, Ländern und Gemeinden. Zur Absicherung eines Web-Servers werden im IT-Grundschutzhandbuch²⁶ u. a. folgende Ziele formuliert:

Abschnitt 4.6
Aufwand 3, Bedeutung 3

- der WWW-Server darf Informationen nur an dazu berechnigte Benutzer weitergeben,
- auf dem WWW-Server werden ausschließlich die für die Weitergabe bestimmten Informationen angeboten,
- die Sicherheit des WWW-Servers kann weder durch berechnigte noch durch unberechnigte Benutzer unterlaufen werden.

Sicherheitsziele

Eine der gravierendsten Gefährdungen eines WWW-Servers ist die Manipulation der bereitgehaltenen Daten. Die Folgen eines Integritätsverlustes durch die Manipulation des Informationsangebots beschränken sich hierbei nicht nur auf den Verlust der Originaldaten. Der Imageverlust, der durch Verbreitung von Falschinformationen entstehen kann, ist in der Regel weitaus schwerwiegender. Dieser ist umso größer, je später die Manipulation bemerkt wird.

Der grundlegendste Schutz vor einer Manipulation der Inhalte des Web-Servers besteht darin, das Ändern von Daten nur solchen Benutzern zu ermöglichen, die

²⁶ Zur sicheren Administration eines WWW-Servers finden sich ausführliche Informationen im IT-Grundschutzhandbuch des BSI, insbesondere in Kapitel 7.5 WWW-Server.

direkt an der Konsole des Rechners arbeiten und Fernzugriffe zu verbieten. Sofern ein Fernzugriff jedoch notwendig ist, sollte der Fernzugriff zum einen über eine verschlüsselte Verbindung erfolgen (s. 4.4, z. B. über ssh, scp oder ähnliche Programme) sowie über eine Firewall abgesichert werden (s. 4.5). Zum anderen sollte der Fernzugriff über ein Benutzerkonto realisiert werden, dessen Rechte aufgabenbezogen eingeschränkt sind. Der Fernzugriff auf administrative Benutzerkonten (Administrator, root o.ä.) sollte vermieden werden.

Auch die Speicherung der Inhalte des Web-Servers auf einer CD-ROM verhindert eine Manipulation der Daten. Dabei muss jedoch berücksichtigt werden, dass die Verwendung von dynamischen Inhalten (z. B. Skripten oder serverseitigen Programmen) eingeschränkt wird sowie die Zugriffe auf diese Informationen langsamer werden. Ebenso können die Inhalte automatisch (mittels eines so genannten Watchdog) mit einem gesicherten Kontrolldatenbestand verglichen werden, der sich nach Möglichkeit in einem anderen Netzsegment als der Web-Server befinden sollte. Die Speicherung des Angebots auf CD-ROM und die Verwendung eines Watchdog können parallel eingesetzt werden.

5 Datenschutz

In diesem Kapitel wird ausführlich darauf eingegangen, welche Themen zu berücksichtigen sind, um ein Angebot datenschutzkonform zu gestalten. Der Bürger erwartet, dass er das Internetangebot der Verwaltung weit gehend anonym nutzen kann, also ohne dass er dabei Angaben zu seiner Person machen muss. Er möchte ausschließen können, dass die im Rahmen der Internetnutzung anfallenden Nutzungsdaten zu Profilen verdichtet werden. Der Umfang der auf dem Web-Server verarbeiteten Daten sollte daher in einer so genannten Datenschutzerklärung veröffentlicht werden. Zur Verbesserung der Transparenz trägt auch bei, in einem Impressum die für das Angebot in redaktioneller Hinsicht verantwortlichen Personen zu benennen.

Rechtsgrundlage für die Gesetzeskonformität von Internetdiensten ist das Teledienstedatenschutzgesetz: Jedes behördliche Web-Angebot beinhaltet, selbst wenn noch kein individueller Datenaustausch zwischen Behörde und Bürger umgesetzt ist, immer auch die Verbreitung von Informationen über das Internet und ist damit als Teledienst im Sinne des § 2 Teledienstegesetzes (TDG) zu qualifizieren. Soweit redaktionelle Inhalte zur Meinungsbildung im Vordergrund stehen, handelt es sich um einen Mediendienst gem. § 2 Abs. 2 Mediendienste-Staatsvertrag (MDStV).

5.1 Transparenz

5.1.1 Anbieter- bzw. Behördenkennzeichnung

Die verantwortliche Behörde trifft als Telediensteanbieter die Pflicht, eine sog. Anbieterkennzeichnung – auch Impressum genannt – auf den Web-Seiten zu veröffentlichen²⁷.

Die Informationspflichten gelten dabei für Teledienste, die geschäftsmäßig angeboten werden – eine Voraussetzung, die immer schon dann vorliegt, wenn die Datenverarbeitung auf eine gewisse Dauer und Wiederholung angelegt ist (entscheidend ist die Intensität des Datenumgangs), wobei **nicht** auf eine Gewinnerzielungsabsicht abgestellt wird²⁸.

Zur Gewährleistung des Selbstbestimmungsrechts der Bürger, die das Behördenangebot zunächst ohne konkrete Absicht aufsuchen, Verwaltungsdienstleistungen in Anspruch nehmen zu wollen, kommt den Informationsverpflichtungen gerade bei diesem ersten Kontakt eine große Bedeutung zu: Der Bürger möchte wissen, mit wem er es auf Anbieterseite zu tun hat, welche juristische und auch natürliche Person hinter dem möglicherweise nicht durch bloßes Durchblättern der Seiten erkennbaren Anbieter tatsächlich steckt, wer Ansprechpartner für die verschiedenen Abteilungen und Zuständigkeitsbereiche ist und, ganz lapidar, welche Tele-

Anbieterkennzeichnung – Sinn und Zweck

Abschnitt 5.1.1
Aufwand 1, Bedeutung 3

²⁷ vgl. § 6 TDG

²⁸ Simitis/Dammann, BDSG § 1 Rn. 228; Schaar, Datenschutz im Internet, Rn. 345

fon- bzw. Faxnummern und welche E-Mail-Adressen zu wählen sind (eine den gesetzlichen Anforderungen entsprechende Anbieter- bzw. Behördenkennzeichnung findet sich in den Mustertexten).

Die Mindestanforderungen für die Behördenkennzeichnung sind nach den gesetzlichen Vorgaben:

Notwendiger Inhalt der Anbieterkennzeichnung

- Name und Anschrift des Diensteanbieters, bei juristischen Personen zusätzlich den Vertretungsberechtigten
- Telefon-, Faxnummern, E-Mail-Adresse
- Umsatzsteuer-Identifikations-Nr., soweit die Behörde Betriebe gewerblicher Art betreibt, vgl. §§ 2, 27a UStG

Die nachfolgend aufgeführten weiteren Inhalte sind nicht notwendiger, d. h. gesetzlich erforderlicher Bestandteil der Behördenkennzeichnung. Im Hinblick auf die Präsentation eines bürgerfreundlichen Web-Auftritts wird die Aufnahme einzelner oder auch sämtlicher dieser Informationen dennoch empfohlen, soweit sie nicht ohnehin schon Bestandteil des Angebots sind (s. 2.2.1):

- eine einfache Darstellung des Organisationsaufbaus mit den für Außenkontakte zuständigen Ansprechpartnern einschließlich der entsprechenden Telefonnummern
- Informationen zur Verantwortlichkeit für eigene Inhalte
- der Hinweis auf die fehlende Verantwortlichkeit für fremde Inhalte
- Urheberrechts- und Copyright-Vermerke
- Anfahrtsskizze zu der bzw. den Behörden

Weiterer Inhalt einer Anbieterkennzeichnung

Um das Web-Angebot besonders nutzerfreundlich zu gestalten und der gesetzlichen Anforderung nachzukommen²⁹ sollte die Behördenkennzeichnung sowohl von der Homepage als auch von allen weiteren Unterseiten aus mit einem einzelnen Mausklick aufrufbar sein. Sie sollte so verständlich bezeichnet werden, dass der durchschnittliche Bürger auf den ersten Blick erkennen kann, was sich dahinter verbirgt. Eingebürgert haben sich hier Bezeichnungen wie „Impressum“, „Wir über uns“ oder auch „Kontakt“.

5.1.2 Datenschutzerklärung/ Privacy Policy

Der Nutzer sollte weiterhin zu Beginn des Nutzungsvorgangs umfassend über die Verarbeitung personenbezogener Daten unterrichtet werden³⁰. Gerade weil er in diesem frühen Stadium häufig noch gar nicht damit rechnet und es für den technischen Laien auch nicht ohne weiteres erkennbar ist, dass bereits mit Aufrufen der Seite(n) personenbezogene Daten erhoben werden (z. B. IP-Adresse, Browsertyp, Uhrzeit und Dauer der Nutzung, Informationen über gesetzte Cookies etc.), ist es

Abschnitt 5.1.2 Aufwand 1, Bedeutung 3

²⁹ vgl. § 6 TDG: Die Anbieterkennzeichnung muss „...leicht erkennbar, unmittelbar erreichbar und ständig verfügbar“ sein.

³⁰ vgl. § 4 Abs. 1 Teledienststedatenschutzgesetz (TDDSG)

aus datenschutzrechtlicher Sicht umso wichtiger, dass der Nutzer darüber informiert wird, wer für die Datenverarbeitung verantwortlich ist und welche Daten erhoben werden. Diesem Umstand tragen die Vorschriften über die Unterrichtung Rechnung.

Mit der Offenlegung der Verarbeitungsabsichten und der Konsequenzen der Erhebung und Speicherung personenbezogener Daten durch den Anbieter eines Dienstes soll erreicht werden, dass der Nutzer zu einem möglichst frühen Zeitpunkt Entscheidungsmöglichkeiten hinsichtlich des weiteren Datenverarbeitungsprozesses erhält.

Die Datenschutzerklärung sollte daher mindestens folgende Themen enthalten:

- eine komplette Auflistung aller Datenarten, die erhoben, gespeichert, verarbeitet und übermittelt werden (aufgeschlüsselt nach Nutzungsdaten, Bestandsdaten, Abrechnungsdaten),
- eine genaue Darstellung des Zwecks der Speicherung und Verarbeitung, wiederum differenziert nach jeweiliger Datenart,
- Informationen darüber, ob die Daten dazu verwendet werden, pseudonyme Profile zu erstellen,
- einen Hinweis darauf, dass der Bürger der Bildung von pseudonymen Nutzungsprofilen widersprechen kann,
- Informationen darüber, ob Cookies oder ähnliche Dateien auf dem Rechner des Bürgers gespeichert werden, zu welchem Zweck diese Cookies dienen und wann diese gelöscht werden,
- soweit umgesetzt, eine Beschreibung, auf welche Weise der gesetzlichen Forderung nach Datensparsamkeit und Datenvermeidung Rechnung getragen wird,
- soweit nicht bereits im Impressum enthalten, eine Mitteilung, ob für die Bereitstellung der Web-Seiten ein externer Dienstleister (Provider) in Anspruch genommen wird, (soweit dies bejaht wird, den Namen, die Adresse und den Ansprechpartner dieses externen Dienstleisters),
- eine Darstellung der Rechte der betroffenen Bürger (s. 5.2.8),
- eine Nennung des behördlichen Datenschutzbeauftragten mit E-Mail-Adresse,
- soweit innerhalb der Behörde festgelegt, Regelfristen für die Löschung der Daten.

Was muss in die Datenschutzerklärung?

Der Diensteanbieter muss den Nutzer „zu Beginn des Nutzungsvorgangs“ über die oben genannten Angaben unterrichten³¹. Es ist somit erforderlich, dass dem Nutzer zumindest gleichzeitig mit Aufruf der Homepage die Gelegenheit gegeben wird, von der Datenschutzerklärung Kenntnis zu nehmen. Dies kann nur dadurch realisiert werden, dass der Link auf die Datenschutzerklärung direkt auf der Homepage, möglichst im „sofort sichtbaren Bereich“ (vgl. hierzu 2.1.2.4) platziert wird. Jederzeitige Abrufbarkeit bedeutet darüber hinaus aber auch, dass von jeder

Platzierung der Datenschutzerklärung

³¹ vgl. § 4 Abs. 1 TDDSG

der Unterseiten die Datenschutzerklärung mit einem Klick erreicht werden muss. Der Link ist somit auch auf jede der Unterseiten zu setzen.

Exkurs: P3P-Standard

Im April 2002 hat das World Wide Web-Konsortium (<http://www.w3.org>) den von internationalen Firmen, Organisationen und Datenschutzbeauftragten aus aller Welt entwickelten Industriestandard P3P (Platform for Privacy Preferences) in der Version 1.0 zur Verwendung in Web-Seiten empfohlen. Die P3P-Spezifikation dokumentiert eine industrieübergreifende Vereinbarung über eine XML-basierte Sprache zur Darstellung von maschinenlesbaren Datenschutzerklärungen. Damit soll es den Nutzern ermöglicht werden, mittels leicht bedienbarer automatisierter Prozeduren die Verwendung ihrer Daten durch die Anbieter der von ihnen besuchten Web-Sites effektiv zu kontrollieren:

Über einen Standard, in dem die Web-Seiten ihre Datenschutzinformationen in der Privacy Policy veröffentlichen, wird ermöglicht, dass der vom Nutzer verwendete und von ihm zuvor mit seinen individuellen Datenschutzpräferenzen konfigurierte Web-Browser die P3P-fähigen Web-Seiten automatisch auslesen und mit den eingestellten Vorgaben vergleichen kann. Weichen die Datenschutzvorgaben der besuchten Seite negativ von den Vorgaben ab (d. h. unterschreitet das Datenschutzniveau der besuchten Seite das vom Nutzer gewünschte Mindestniveau), wird der Nutzer darauf hingewiesen und kann ggf. die Verbindung zum Anbieter abbrechen.

Mit den nachfolgend genannten "P3P-Generatoren" können solche Standard-Erklärungen erstellt werden:

- IBM P3P Policy Editor (<http://www.alphaworks.ibm.com/tech/p3peditor>)
- PrivacyBot.com (<http://www.privacybot.com/>)
- P3Pedit (www.policyeditor.com)
- Customer Paradigm's P3P Privacy Policy Creation (<http://www.customerparadigm.com/p3p-privacy-policy3.htm>)

Obwohl allein durch die P3P-Kompatibilität materiell-datenschutzrechtlich noch kein Fortschritt erzielt wird (es handelt sich, wie soeben aufgezeigt, im Wesentlichen um Absichtserklärungen des Anbieters), ist damit zu rechnen, dass sich P3P als Quasi-Standard für Datenschutzerklärungen mittelfristig etablieren wird. In diesem Zusammenhang wird in die jeweiligen neuen Browserversionen P3P komfortabel integriert sein. Aus diesem Grunde wird an dieser Stelle empfohlen, die Datenschutzerklärung mittelfristig P3P-konform zu gestalten. Um dies programmiertechnisch umzusetzen, ist die Verwendung einer der genannten Generatoren zu empfehlen. In jedem Fall ist bei der P3P-konformen Gestaltung der Datenschutzerklärung darauf zu achten, dass nach wie vor die rechtlichen Anforderungen des TDDSG eingehalten werden: Für deutsche Anbieter ist dies nach wie vor der einzig verbindliche Maßstab.

5.1.3 Informationen über Weitervermittlung

§ 4 Abs. 5 TDDSG sieht vor, dass der Anbieter den Bürger darüber informieren muss, wenn er ihn über einen Verweis auf seinen Seiten an einen anderen Diensteanbieter weiter vermittelt. Eine solche Weitervermittlung findet immer dann statt, wenn der Bürger über einen Link auf ein Angebot geleitet wird, für das ein anderer Anbieter im Sinne des TDG verantwortlich ist. Hintergrund auch dieser Informationspflicht ist, dem Bürger eine höchstmögliche Transparenz zu gewährleisten: Wenn sich die Aufmachung der aufgerufenen Seiten nicht entscheidend verändert, merkt der durchschnittliche Bürger oft nicht, dass er über mehrere Links auf dem Angebot eines anderen Anbieters gelandet ist. Wenn der Anbieter seiner Informationspflicht nicht nachkommt, wird die Weitervermittlung für den Bürger erst dadurch ersichtlich, dass sich die URL der aufgerufenen Seite geändert hat. Selbst dies muss dem durchschnittlichen Bürger aber nicht ohne weiteres auffallen, wenn seine Aufmerksamkeit nur auf den Browserinhalt, nicht aber auf das Adress- bzw. Statusfenster gerichtet ist. Folge dieser unbemerkten Weiterleitung wäre, dass Nutzungsdaten in diesem Fall ohne Kenntnis des Bürgers bei weiteren Anbietern erhoben und verarbeitet würden. Aus diesem Grund ist der Anbieter gesetzlich dazu verpflichtet, den Bürger auf eine solche Weiterverweisung, beispielsweise auf so genannte Web-Services, in geeigneter Form hinzuweisen.

Abschnitt 5.1.3
Aufwand 1, Bedeutung 2

Da die Weitervermittlung für den Bürger als solche erkennbar sein muss, ist der Hinweis so zu gestalten, dass der durchschnittliche Nutzer ohne weiteres erkennt, dass es sich bei dem Link um eine Weiterleitung zu einem Angebot handelt, für das ein anderer Diensteanbieter verantwortlich ist. Realisiert werden kann dies entweder durch einen zusätzlichen Erläuterungstext, der sich eindeutig auf den Link bezieht, oder auch durch ein so genanntes Quick-Info, also ein Hinweiskärtchen, welches sich öffnet, sobald der Mauszeiger auf den Link zeigt. Sowohl Erläuterungstext als auch Quick-Info enthalten idealerweise den Namen des Anbieters bzw. Servers, zu dem weitervermittelt wird.

Was muss der Nutzer über die Weitervermittlung wissen?

5.2 Materielle Rechtmäßigkeit der Datenverarbeitung

5.2.1 Erhebung, Speicherung und Auswertung von Nutzungsdaten

Nutzungsdaten sind nach § 6 TDDSG solche, die zur Inanspruchnahme oder zur Abrechnung des Dienstes erhoben werden dürfen, insbesondere

- Merkmale zur Identifikation des Bürgers,
- Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und
- Angaben über die vom Bürger in Anspruch genommenen Teledienste.

Der Diensteanbieter darf solche Nutzungsdaten nur erheben und verarbeiten, soweit dies für die Inanspruchnahme von Telediensten und zu Abrechnungszwecken

Abschnitt 5.2.1
Aufwand 1, Bedeutung 3

Zulässigkeit der Speicherung von Nutzungsdaten

erforderlich ist. Da die Internet-Plattformen der Verwaltung in aller Regel jedoch für den Bürger kostenfrei nutzbar sind und somit keine Abrechnungsdaten benötigt werden, dürften daher gemäß § 6 Abs. 4 TDDSG gar keine Nutzungsdaten bei den Behörden gespeichert werden; die Daten sind unmittelbar nach der Beendigung der Inanspruchnahme des Web-Auftritts zu löschen.

In diesem Zusammenhang soll ausdrücklich darauf verwiesen werden, dass auch IP-Adressen ein personenbezogenes Datum sind. Zwar stellen dynamisch vergebene IP-Adressen ein Pseudonym dar, das nur unter Mitarbeit des Internet-Providers, über den der Zugang des Bürgers zum Internet erfolgt, einer konkreten Person zugeordnet werden kann. Statisch vergebene IP-Adressen erlauben es jedoch, sofern der Internetzugang direkt und nicht über einen Proxy-Server erfolgt, konkret den Rechner und somit auch den Benutzer zu ermitteln, der auf den Web-Server der Verwaltung zugreift. Da aber nicht ermittelt werden kann, ob es sich um eine dynamisch vergebene oder statische IP-Adresse handelt, muss auf die IP-nummernbezogene Speicherung von Nutzungsdaten vollständig verzichtet werden.

Der Verzicht auf eine IP-nummernbezogene Speicherung von Nutzungsdaten bezieht sich allerdings nicht auf den Betrieb von Firewallsystemen. Um den Gefahren begegnen zu können, denen ein Web-Server ausgesetzt ist, ist eine begrenzte Protokollierung erforderlich; die Protokollierung ist quasi Gegenstand der mit dem Einsatz einer Firewall verbundenen Dienstleistung. Von den Datenschutzbeauftragten des Bundes und der Länder wird daher empfohlen, zum einen lediglich diejenigen Verbindungen zu protokollieren, die aufgrund der Filterregeln vom Firewall geblockt werden.³² Zum anderen können auch diejenigen Dienste wie beispielsweise telnet oder ftp protokolliert werden, die zwar von der Firewall weiter transportiert werden, die jedoch grundsätzlich als sicherheitskritisch einzustufen sind (vgl. 4).

5.2.2 Erhebung, Speicherung, Nutzung von Bestandsdaten

Nach § 5 Abs. 1 TDDSG sind Bestandsdaten diejenigen Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit dem Bürger über die Inanspruchnahme von Telediensten erforderlich sind (Grunddaten des Vertragsverhältnisses). Ausschlaggebend für den Umfang der zulässigerweise erhobenen Bestandsdaten ist der Zweck des jeweils entstehenden Vertragsverhältnisses. Zu den Bestandsdaten bei Tele- und Mediendiensten gehören üblicherweise die Personalien, sowie bei kostenpflichtigen Diensten die Daten über den Abrechnungsmodus. Weitere Bestandsdaten sind, je nach Art und Ausgestaltung des Angebotes, Angaben über die Bankverbindung, Zugangskennungen (auch Pseudonyme) sowie E-Mail-Adressen. Aufgrund der Vielzahl der im Rahmen von Verwaltungsdienstleistungen möglichen Zwecke kann an dieser Stelle keine weitere Eingrenzung von zulässiger- oder unzulässigerweise erhobenen Bestandsdaten vorgenommen werden.

Abschnitt 5.2.2
Aufwand 1, Bedeutung 3

³² zu Einzelheiten bzgl. der Firewall-Filterregeln vgl. Modul „Sicherer Internet-Auftritt im E-Government“ (dort Abschnitte 5.2 und 5.3)

Da sich die Zulässigkeit der Erhebung der Bestandsdaten danach richtet, ob diese für das Vertragsverhältnis mit dem Bürger erforderlich sind, ist eine Erhebung dieser Daten **vor** Eingehen eines solchen Vertragsverhältnisses unzulässig. In keinem Fall dürfen daher vom Bürger Bestandsdaten schon beim bloßen Sichten des Angebotes oder kostenlosen Download von Formularen abgefordert werden. Erst wenn die Dienstleistung ohne die Angabe der Personalien und weiterer Bestandsdaten nicht erbracht werden kann, ist die Erhebung zulässig. Diese Anforderung besteht als strenge Zweckbindung über den gesamten Zeitraum von der Erhebung der Daten bis zu deren Löschung: die Daten dürfen nur für den Zweck gespeichert und verarbeitet werden, zu dem sie erhoben worden sind.

Zulässigkeit der Speicherung von Bestandsdaten

5.2.3 Einwilligung des Bürgers

Jede Erhebung und Verarbeitung personenbezogener Daten außerhalb der gesetzlich ausdrücklich zugelassenen Zwecke bedarf auch im Bereich der Tele- und Mediendienste der Einwilligung des Betroffenen, eine solche Einwilligung kann sich hier ausschließlich auf die erwähnten Bestands- und Nutzungsdaten beziehen.

Einwilligung und Widerruf bei der Datenerhebung

§ 3 Abs. 3 TDDSG erlaubt elektronische Einwilligungen, sofern der Diensteanbieter sicherstellt, dass

Abschnitt 5.2.3 Aufwand 2, Bedeutung 4

- „1. sie nur durch eine eindeutige und bewusste Handlung des Bürgers erfolgen kann,
2. die Einwilligung protokolliert wird und
3. der Inhalt der Einwilligung jederzeit vom Bürger abgerufen werden kann.“

Der Diensteanbieter hat den Bürger dabei vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Das TDDSG schreibt kein besonderes Verfahren vor, nach dem die Einwilligung zu erteilen ist. So kann die Einwilligung sowohl online als auch per E-Mail erfolgen.

Für die Einwilligung muss sichergestellt sein, dass der Betroffene, dessen Daten erhoben, verarbeitet oder genutzt werden sollen, diese durch eine bewusste Handlung abgibt und dass er tatsächlich Urheber der Einwilligung ist. Weiterhin muss der Inhalt der elektronischen Einwilligung für den Bürger jederzeit abrufbar sein. Er soll in die Lage versetzt werden, den Inhalt einer von ihm abgegebenen Einwilligung auch dann zu erfahren, wenn ihm nur bekannt ist, welchem Diensteanbieter gegenüber er sie abgegeben hat. Da der Diensteanbieter die Einwilligung protokollieren muss, hat er dem Bürger im Übrigen Auskunft über die Tatsache und den Inhalt der Einwilligung zu erteilen, etwa wenn der Bürger sich nicht mehr mit Sicherheit daran erinnern kann, ob er eine Einwilligung erteilt hat. Jederzeit abrufbar ist eine Einwilligung dann, wenn der Bürger auf sie rund um die Uhr über das Internet zugreifen kann. Die setzt jedoch wiederum entsprechende Authentisierungsmechanismen zum Zugriff auf die erteilte Einwilligung voraus.

Einwilligung nur durch bewusste Handlung

Dem Anspruch eines fortschrittlichen Web-Auftritts gerecht wird die Einwilligung in elektronischer Form mittels des Einsatzes einer elektronischen Signatur: Die

Einwilligung – wie sollte sie umgesetzt werden?

verantwortliche Stelle könnte dem Bürger den Text der Einwilligung per E-Mail zusenden, dieser sendet diese E-Mail mit seiner Einverständniserklärung zurück. Eine weitere, wenngleich hinsichtlich der Sicherung der Authentizität des Bürgers schwächere Möglichkeit, wäre die Einblendung eines Bildschirmfensters mit dem Inhalt der Einwilligung: Durch Anklicken eines eindeutig beschrifteten Auswahl-feldes bestätigt der Bürger seine Einwilligung – im Anschluss daran wird ihm per E-Mail noch eine Bestätigung zugesandt. Dies dient nicht nur der Transparenz für den Bürger, sondern ermöglicht auf diese Weise auch die Protokollierung der Einwilligung durch die verantwortliche Stelle.

Exkurs: Zulässigkeit der Erhebung einwilligungsrelevanter Daten

Die Verwendung personenbezogener Daten der Bürger für Zwecke der Werbung, Marktforschung und zur bedarfsgerechten Gestaltung der Dienste dürfte für Behörden und die Verwaltung allgemein – mit Ausnahme der Verwendung für die bedarfsgerechte Gestaltung der Dienste – ohnehin unzulässig sein. Vor dem Hintergrund der Grundsätze zur Erforderlichkeit der Datenerhebung zur Aufgabenerfüllung, die sich im Wesentlichen an der *Zuständigkeit* der jeweiligen Behörde orientiert, wird deutlich, dass Werbungs- und Marktforschungszwecke gerade nicht in den Zuständigkeitsbereich der Verwaltung fallen. Die nach dem TDDSG für privatrechtliche Anbieter (mit Einwilligung) zulässigen Verwendungsarten werden insoweit für die Verwaltung durch die speziellen öffentlich-rechtlichen Zuständigkeitsbestimmungen eingeschränkt.

5.2.4 Übermittlung von Bestands- und Nutzungsdaten an Dritte

Nutzungsdaten, die bei der Inanspruchnahme des behördlichen Web-Angebotes erhoben wurden, dürfen ohne Einwilligung des Betroffenen nur dann an Dritte übermittelt werden, wenn diese als Abrechnungsdaten für die Ermittlung einer Entgeltabrechnung erforderlich sind (Nutzungsdaten werden durch die Notwendigkeit, mit Ihnen eine Entgeltabrechnung vorzunehmen, zu Abrechnungsdaten, vgl. § 6 Abs. 4 TDDSG). Dies kommt in der Regel bei Web-Angeboten der Verwaltung nicht vor, da die Nutzung dieses Angebots in Form des bloßen Seitenabrufs in der Regel kostenfrei ist. Anderenfalls dürfen diese Abrechnungsdaten an Dritte zum Zweck der Abrechnung übermittelt werden.

Bestandsdaten dürfen dagegen ohne ausdrückliche Einwilligung des Bürgers überhaupt nicht an Dritte übermittelt werden. Selbst die Zweckänderung, also die Nutzung für andere als die bei Erhebung der Daten festgelegten Zwecke, bedarf nach überwiegender Auffassung der vorherigen Einwilligung des Bürgers³³.

Abschnitt 5.2.4
Aufwand 1, Bedeutung 2

³³ BT-Drs. 14/6098, 29; P. Schaar, Datenschutz im Internet, Rn. 396-398

5.2.5 Pseudonyme Auswertung von Bestands- und Nutzungsdaten

Zwar dürfen Anbieter von Telediensten für Zwecke der Werbung, Marktforschung oder bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile unter einem Pseudonym (also einem Kennzeichen, welches zwar zur Bestimmung des Betroffenen herangezogen werden kann, ihn aber nicht unmittelbar identifiziert) erstellen³⁴ – dies jedoch nur dann, wenn der Nutzer dieser speziellen Verwendung seiner Daten nicht widerspricht.

Was sind Nutzungsprofile?

Ein solcher Widerspruch ist ihm naturgemäß nur möglich, wenn er auf die Profilerstellung – i.d.R. im Rahmen der Datenschutzerklärung – auch explizit hingewiesen wird (so genannte Opt-out-Lösung). Soweit eine Profilerstellung überhaupt erfolgen soll, ist demnach ein ausdrücklicher Hinweis auf das Widerspruchsrecht in der Datenschutzerklärung obligatorisch (s. 5.1.2).

Abschnitt 5.2.5
Aufwand 1, Bedeutung 3

Soweit eine – pseudonyme – Profilerstellung für die Verwaltung nicht aus zwingenden Gründen erforderlich ist, sollte davon abgesehen werden, solche Profile (in welcher Form auch immer) zu erstellen: Jegliche Profilbildung stößt bei dem Bürger auf Skepsis hinsichtlich der weiteren Verwendung. Wengleich viele Bürger kommerzielle Angebote trotz der Kenntnis oder nur der Befürchtung nutzen, Profile zu hinterlassen, erfolgt dies in der Regel aufgrund einer freien Entscheidung für den einen und damit gegen den anderen Anbieter. Oftmals nehmen Bürger eine solche Einschränkung ihres Persönlichkeitsrechts hin, wenn die entsprechende Gegenleistung des Anbieters (der Preis für eine Ware oder Dienstleistung z. B.) überzeugt.

Für das Verwaltungshandeln besteht kein solcher Markt: Der Bürger hat keine Wahl, von welcher Behörde er die gewünschte Verwaltungsdienstleistung erhält, er ist aufgrund unterschiedlicher Vorgaben (z.B. Wohnsitz) auf einen „Anbieter“ festgelegt. Würde er vor dem Hintergrund dieser monopolartigen Anbieterposition mit einer Profilerstellung konfrontiert, hätte dies einen Zuwachs an Misstrauen gegenüber der Verwaltung allgemein zur Folge.

Für den Fall, dass auf eine Profilerstellung nicht verzichtet werden kann, muss der Anbieter von Gesetzes wegen sicherstellen, dass die Nutzungsprofile nicht mit den Daten über den Träger des Pseudonyms zusammengeführt werden, vgl. § 4 Abs. 4 Nr. 6 TDDSG. Mithilfe des zentralen Web-Servers der Behörde dürfen keine Bewegungs- bzw. Nutzungsprofile einzelner Bürger erstellt und unterschiedliche Verwaltungsvorgänge nicht unbefugt zusammengeführt werden. Darüber hinaus ist zu beachten, dass Nutzungsprofile nur aus den zulässiger Weise erhobenen Nutzungsdaten (zum Umfang der zulässigen Daten, s. 5.2.1) erstellt werden dürfen, also nur aus denjenigen Daten, die bei der Erbringung des Dienstes ohnehin angefallen sind. Auf den in diesem Fall obligatorischen Hinweis auf das Widerspruchsrecht des Bürgers und die Information, wie es auszuüben ist, ist bereits hingewiesen worden (s. 5.1.2). Wird dieser Hinweis versäumt, ist nicht nur die Unterrichtung unvollständig; die Bildung von Nutzungsprofilen ist ohne diesen Hinweis allgemein unzulässig.

In welchem Umfang dürfen Nutzungsprofile erstellt werden?

³⁴ vgl. § 6 Abs. 3 TDDSG

Hinzuweisen ist abschließend, dass IP-Adressen in diesem Zusammenhang keine Pseudonyme sind, sondern „normale“ personenbezogene Daten. Über das bereits genannte Verbot der Speicherung dieser IP-Adressen über den Zeitraum der Nutzung hinaus bedeutet dies, dass aus diesen Daten auch keine (vermeintlich) pseudonymen Profile erstellt werden dürfen.

5.2.6 Speicherung und Löschung von E-Mails

Für die Frage der Zulässigkeit der Speicherung von E-Mails gelten dieselben Voraussetzungen wie für die Speicherung sonstiger personenbezogener Daten, nämlich im Wesentlichen die allgemeinen Vorschriften des Bundes- bzw. der Landesdatenschutzgesetze. Die speziellen datenschutz- und kommunikationsrechtlichen Vorgaben der Teledienstedatenschutzverordnung (TDSV) gelten in diesem Bereich **nicht**, da diese Vorgaben (die z. B. die Höchstspeicherdauer von Verbindungsdaten betreffen) nur gegenüber Telekommunikationsdiensteanbietern gelten, vgl. §§ 1 und 2 TDSV. Behörden und Verwaltungen treten dem Bürger gegenüber zwar als Telediensteanbieter, jedoch nicht als Anbieter im Sinne des TDSV auf, sondern sind – ebenso wie der Bürger – Beteiligte an der Telekommunikation.

Abschnitt 5.2.6
Aufwand 1, Bedeutung 4

Das Speichern von E-Mails ist somit zulässig, wenn und solange es zur Erfüllung der Aufgaben der zuständigen Stelle erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind, § 14 Abs. 1 BDSG³⁵.

5.2.7 Cookies, Web-Bugs und ähnliche nutzeridentifizierende Techniken

Ein Web-Server kann, sofern es die Einstellungen des WWW-Browsers zulassen, eine Nachricht (Cookie) auf dem Client in Form einer Textdatei speichern. Cookies werden, meist vom durchschnittlichen Bürger unbemerkt, bei jedem weiteren Besuch der Internetseite an den jeweiligen Web-Server gesandt und dort zur Erhebung demografischer Informationen oder zur Identifikation des Bürgers für ein personalisiertes Informationsangebot verwendet.

Abschnitt 5.2.7
Aufwand 2, Bedeutung 3

In HTML-Seiten können auch externe Inhalte, die sich auf einem weiteren WWW-Server befinden, eingebunden werden. Der Bürger ruft hierbei zwei verschiedene Informationsangebote von zwei verschiedenen WWW-Servern ab. Sofern die externen Informationen nicht als solche gekennzeichnet und schwer erkennbar sind, werden sie auch als Web-Bugs bezeichnet.

Exkurs: Datenschutz versus Benutzerfreundlichkeit

Bei der datenschutzrechtlichen Beurteilung über die Verwendung oder den Verzicht auf die Verwendung von Cookies muss zunächst auf eine kaum vermeidbare Inkongruenz innerhalb dieses Moduls hingewiesen werden: Während Cookies als für die Bedienerfreundlichkeit durchaus vorteilhaft dargestellt werden, ist die

³⁵ Weitere Zulässigkeitsvoraussetzungen nach § 14 Abs. 2 BDSG sind u.a. das Bestehen einer speziellen Rechtsvorschrift, die Einwilligung des Betroffenen, ein anzunehmendes offensichtliches Interesse des Betroffenen oder die allgemeine (öffentliche) Zugänglichkeit der Daten.

Verwendung solcher lokal auf dem Rechner des Bürgers gespeicherter Dateien aus datenschutzrechtlicher Sicht als eher kritisch anzusehen. Die Wiedererkennung des Bürgers und seiner zuletzt in Anspruch genommenen Dienste macht die Nutzung ohne Frage komfortabler, bedeutet aber ebenso eine teilweise Preisgabe seiner Anonymität. Das Beispiel von Cookies macht somit die unterschiedlichen Beurteilungsmaßstäbe der Nutzerfreundlichkeit einerseits und vorbildlichem Datenschutz andererseits deutlich! Für die Lösung dieses Konflikts hat sich bisher kein Idealweg gefunden – aus datenschutzrechtlicher Sicht ist die Verwendung von Cookies nicht zu empfehlen.

Cookies –
Pro und Contra

Der Grund, warum Cookies aus datenschutzrechtlicher Sicht als problematisch betrachtet werden, liegt darin, dass durch das Setzen dieser Cookies nutzeridentifizierende Dateien – wenn auch anonym oder in pseudonymer Form - auf der Festplatte des Bürgers gespeichert werden, ohne dass dieser – jedenfalls als durchschnittlicher Bürger – hiervon etwas weiß. Dieses Vorgehen widerspricht damit dem Grundrecht auf informationelle Selbstbestimmung (als Teil des allgemeinen Persönlichkeitsrechts), wonach jeder Einzelne selbst bestimmen soll, wer welche Daten über ihn speichert.

Die hierzu einschlägige gesetzliche Regelung (§ 4 Abs. 1 S. 1 TDDSG) sieht vor, dass der Anbieter den Bürger

„zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten [...] unterrichten...“

muss. Die Umsetzung dieser Vorgabe ist jedoch schwierig, denn nach der gängigen Anbieterpraxis werden Cookies schon unmittelbar bei dem ersten Aufruf der entsprechenden Seite auf der Festplatte des Bürgers abgelegt. Eine gesetzeskonforme Unterrichtung hierüber muss also den Bürger zumindest „gleichzeitig“ mit dem ersten Seitenaufruf über die Cookieverwendung informieren, z. B. in Form eines Pop-up-Fensters zusätzlich zur jederzeit abrufbaren Unterrichtung. Dies gilt sogar dann, wenn Cookies noch keinen direkten Personenbezug aufweisen, sondern erst später zur Identifizierung des bis dahin noch pseudonymen Bürgers führen können. § 4 Abs. 1 Satz 2 TDDSG sieht vor, dass auch für diese (noch) nicht personenbezogenen Daten eine entsprechende Unterrichtung erfolgen muss:

„Bei automatisierten Verfahren, die eine spätere Identifizierung des Bürgers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Bürger zu Beginn dieses Verfahrens zu unterrichten.“

Der Anbieter muss dementsprechend in jedem Fall die (zeitlich) erste Möglichkeit wählen, den Bürger über seine Cookie-Politik aufzuklären. Diese Information muss jedoch darüber hinaus auch jederzeit abrufbar sein, da insoweit die gleiche Anforderung gilt, wie für die Datenschutzerklärung (in der Regel werden die Datenschutzerklärung und die Information über die Cookies in einer Erklärung zusammengefasst). Der Link muss somit nicht nur von der Startseite, sondern von jeder Unterseite ebenfalls auf die Unterrichtung verweisen.

Die Verwendung von Cookies steht in engem Zusammenhang mit der Bildung von Nutzerprofilen, bzw. ist in aller Regel Voraussetzung und Mittel zur Erstel-

In welcher Form
muss über Cookies
informiert werden?

Inhalt des Widerspruchsrechts

lung solcher Profile (s. 5.2.5) . Für die Bestimmung des notwendigen Inhalts der Unterrichtung über die Verwendung von Cookies ist daher relevant, ob und in welchem Umfang, vor allem zu welchem Zweck solche Profile erstellt werden und was mit den erzeugten Profilen geschieht. Soweit Nutzungsprofile unter einem Pseudonym erstellt werden, hat der Bürger hiergegen das bereits erwähnte Widerspruchsrecht³⁶. In der Unterrichtung müssen mindestens Informationen über

- den technischen Vorgang (was genau passiert auf dem System des Bürgers, was wird wie lange gespeichert),
- die Verwendung der Cookie-Informationen in der Behörde,
- die Bildung von Nutzungsprofilen (soweit zutreffend),
- den Zweck und die Verwendung der Profile,
- die Speicherdauer,
- das Widerspruchsrecht des Bürgers und wie es auszuüben ist,

enthalten sein. Die Ausübung des Widerspruchsrechts sollte im übrigen ebenso unter einem Pseudonym ermöglicht werden; hierfür bietet sich die Verwendung sog. „Opt-out-Cookies“ an: in diesem Fall hat das auf dem Rechner des Bürgers platzierte Opt-out-Cookie eine datenschutzrechtlich positive Funktion, nämlich dem Cookie-Absender mitzuteilen, dass der Bürger das Setzen profilbildender Cookies explizit nicht wünscht.

5.2.8 Wahrung der Rechte der betroffenen Bürger

Zu einem bürgerfreundlichen und datenschutzrechtlich vorbildlichen Web-Auftritt gehört eine klare, leicht auffindbare und verständliche Regelung, wie betroffene Bürger ihre gesetzlich verankerten Rechte auf Auskunft, Benachrichtigung, Berichtigung, Sperrung und Löschung (§§ 19 - 20 BDSG bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze) ihrer Daten wahrnehmen können.

Wesentlicher Teil dieser Regelung ist dabei die Information bzw. die Unterrichtung des Betroffenen über das Bestehen und den Umfang dieser Rechte, denn vielen Bürgern sind diese Rechte oftmals unbekannt. Der datenschutzfreundliche Web-Auftritt zeichnet sich daher durch eine offene, aktive Information des Bürgers über seine Rechte sowie eine möglichst einfache technische Umsetzung dieser Rechte aus. Dies beinhaltet auch, den betroffenen Bürgern von sich aus – d. h. ohne seine vorherige Anfrage – zu benachrichtigen, wenn Daten über ihn erhoben werden, ohne dass er hiervon Kenntnis bekommt (vgl. § 19a BDSG). Ein gut organisiertes Auskunftsmanagement kann damit für viele Behörden zum Aushängeschild für vorbildlichen Datenschutz werden.

Es ist sinnvoll, die Informationen über das Bestehen, Umfang und Wahrnehmung der Betroffenenrechte ebenfalls mit in die Datenschutzerklärung aufzunehmen. Hier bietet es sich an, einen separaten Teil ausschließlich den Betroffenenrechten zu widmen; dieser beinhaltet dann mindestens Informationen über

Wozu Betroffenenrechte?

**Abschnitt 5.2.8
Aufwand 1, Bedeutung 4**

Information der Betroffenen über ihre Rechte

³⁶ vgl. § 6 Abs. 3 TDDSG

- die Rechte selbst,
- die Voraussetzungen, unter denen sie geltend gemacht werden können (einfache, verständliche Darstellung),
- die Form, in der sie im konkreten Web-Auftritt geltend gemacht werden können,
- die Tatsache, dass die Auskunft unentgeltlich erfolgt.

Damit die Bürger ihre Rechte wahrnehmen können, bietet es sich an, ein Web-Formular zu Verfügung zu stellen. Dieses Formular sollte möglichst per SSL verschlüsselt werden. Auch hier sollten Mechanismen zur Verfügung gestellt werden, damit sich der Bürger gegenüber der Verwaltung entsprechend authentisieren kann.

Die dem Betroffenen erteilte Auskunft beinhaltet - in Abhängigkeit von der konkreten Anfrage - im allgemeinen Informationen über:

- den Umfang der Daten einschließlich solcher, die unter Pseudonym gespeichert sind,
- die Herkunft der Daten,
- die Empfänger, denen die Daten übermittelt werden (soweit eine Übermittlung erfolgt),
- den Zweck der Speicherung,
- die voraussichtliche Dauer der Speicherung,
- Cookies, die beim Betroffenen gespeichert werden und eine Identifizierung des Betroffenen ermöglichen (soweit dies erfolgt).

Zusätzlich zu diesen Informationen sollte obligatorischer Bestandteil jeder Auskunft auch die E-Mail-Adresse des für den Datenschutz Verantwortlichen sein.

5.3 Datensparsamkeit

Nach dem neuen Bundesdatenschutzgesetz sollen sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel ausrichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen³⁷. Bei Telediensten geht die Forderung nach Datensparsamkeit sogar so weit, dass der Diensteanbieter dem Bürger die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter einem Pseudonym ermöglichen muss, soweit dies technisch möglich und zumutbar ist³⁸. Ob dieser Pflicht zur Umsetzung von Maßnahmen zur Datenvermeidung und zur Datensparsamkeit nachzukommen ist (z. B. nachträgliche Pseudonymisierung), ist konkret abzuwägen: steht der finanzielle

Abschnitt 5.3
Aufwand 3, Bedeutung 3

³⁷ vgl. § 3a BDSG; entsprechende Regelungen finden sich auch in den Landesdatenschutzgesetzen von Berlin, Brandenburg, Hamburg, Niedersachsen und Schleswig-Holstein wieder. Es ist damit zu rechnen, dass bei der künftigen Novellierung von weiteren Landesdatenschutzgesetzen Regelungen zur Datenvermeidung aufgenommen werden.

³⁸ vgl. § 4 Abs. 6 TDDSG

und personelle Aufwand (zur Erreichung von Datensparsamkeit) in einem angemessenen Verhältnis zum Interesse des Betroffenen an einer geringstmöglichen Datenerhebung?

Dass nicht für jedes Verwaltungshandeln eine Identifikation des Bürgers erforderlich ist, können zwei Beispiele verdeutlichen:

1. Datensparsamkeit durch die Ermöglichung anonymer Bezahlung:

Als Gegenleistung für Verwaltungsleistungen müssen Bürger Gebühren zahlen bzw. Auslagen erstatten. Die Notwendigkeit der Bezahlung von Verwaltungsleistungen darf jedoch nicht dazu führen, dass sich die Bürger allein aus diesem Grund gegenüber der Verwaltung identifizieren müssen. Im Übrigen ist darauf zu achten, dass durch die Bezahlungsfunktion keine unzulässige Zusammenführung von personenbezogenen Daten aus verschiedenen Verwaltungsbereichen stattfindet. Für das Internet stehen inzwischen funktionsfähige Verfahren zur Verfügung, über die sich die Bezahlung elektronischer Dienstleistungen anonym und sicher abwickeln lassen. Besondere Bedeutung kommt dabei der Verwendung von anonymen bzw. pseudonymen Prepaid-Verfahren zu, die die Bezahlung mittels Abbuchen von einer Chipkarte (Guthabekarte, Beispiel: Geldkarte) ermöglichen. Bei der Abbuchung über solche Verfahren ist keinerlei Personenbezug erforderlich, gleichwohl hat diese Anonymität ihren Preis: auf die vergleichsweise hohen Anfangsinvestitionen ist bereits eingegangen worden (s. 3.3.2).

Beispiele für den sparsamen Umgang mit Daten

2. Ermöglichung pseudonymer Nutzung:

Angebote, die zwar eine direkte Kommunikation zwischen den Bürgern und der Verwaltung voraussetzen, etwa hinsichtlich der Zuordnung zu einer bestimmten Gruppe, bei denen jedoch eine namentliche Kenntnis der Betroffenen nicht erforderlich ist, sollten von den Bürgern auch unter Pseudonym genutzt werden können. Ein Anwendungsfall ist z. B. die Bereitstellung eines erweiterten Vorlesungsverzeichnisses, zu dem allein die Mitglieder einer Hochschule Zugang haben sollen.

Angesichts dieser Beispiele ist für jede Maßnahme, die auf den ersten Blick die Erhebung personenbezogener Daten erforderlich macht, zu prüfen, ob es zur Erfüllung der Aufgabe nicht auch ausreichend ist, den Betroffenen unter einem Pseudonym zu führen oder ob eine Identifikation des Betroffenen überhaupt erfolgen muss.

6 Verantwortlichkeit für Inhalte

In diesem Kapitel wird ausführlich auf die Verantwortlichkeit für eigene und fremde Internet-Inhalte eingegangen, die auf dem Web-Server der Behörde präsentiert werden. Dabei sind auch Aspekte des Jugendschutzes zu berücksichtigen. Klar definierte Verantwortlichkeiten sind eine Voraussetzung dafür, dass auf den Internetseiten der Verwaltung möglichst keine rechtswidrigen oder jugendgefährdenden Inhalte veröffentlicht werden.

6.1 Verantwortlichkeit für eigene und fremde Inhalte

Die Behörde ist als Anbieter eines Teledienstes für eigene Informationen (Inhalte) grundsätzlich selbst verantwortlich³⁹. Eigene Informationen sind zum einen diejenigen, die man selbst aussucht, um sie im Netz anzubieten. Dies können Inhalte sein, die die Behörde selbst erstellt hat oder aber solche, die zwar aus anderen Quellen stammen (Büchern, Druckschriften, anderen Internet-Angeboten) jedoch aus dem Zusammenhang, in den sie gestellt bzw. innerhalb des Angebotes eingebunden werden, ersichtlich ist, dass sie Bestandteil des eigenen Angebots werden sollen.

Abgrenzung eigene / fremde Inhalte

Selbst ein Link zu anderen Inhalten kann diese zu eigenen Inhalten im Sinne dieser Bestimmung machen, wenn der Zusammenhang darauf schließen lässt. Auch ein Hinweis darauf, sich von dem Inhalt distanzieren zu wollen, kann im Einzelfall nicht ausreichen, wenn sich aus dem Gesamtzusammenhang eine andere Interpretation aufdrängt. Da die Grenze hier fließend ist, sollte vor Einbindung fremder Links zuvor immer das Zielangebot auf Rechtskonformität überprüft werden.

Abschnitt 6.1 Aufwand 2, Bedeutung 3

Ausnahmen vom soeben dargestellten Grundsatz der eigenen Verantwortlichkeit gelten

- für fremde Informationen, die Anbieter in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, sofern sie
 - die Übermittlung nicht veranlasst,
 - den Adressaten der übermittelten Informationen nicht ausgewählt und
 - die übermittelten Informationen nicht ausgewählt oder verändert haben (§ 9 Abs.1 TDG),
- für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung der fremden Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, sofern die Anbieter
 - die Informationen nicht verändern,
 - die Bedingungen für den Zugang zu den Informationen beachten,

Transport fremder Inhalte (Providing)

Zwischenspeicherung fremder Inhalte (Caching)

³⁹ zentrale Norm ist hier der § 8 TDG sowie § 6 MStV für redaktionelle Inhalte

- die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
 - die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und
 - unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat (§ 10 TDG),
- für fremde Informationen, die Anbieter für einen Nutzer speichern, sofern
 - sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder Information offensichtlich wird, oder
 - sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben (§ 11 TDG).

**Speicherung
fremder Inhalte
(Hosting)**

Die Wirkungsweise dieser Ausnahmen kann man untechnisch mit der eines Filters vergleichen: Die Vorschriften (§ 9-11 TDG) können eine Verantwortlichkeit im zivil- oder strafrechtlichen Bereich nicht begründen oder erweitern, sondern nur auf allgemeine Vorschriften verweisen, aus denen sich eine Verantwortlichkeit ergibt.

Als Leitfaden, welche Art von Inhalten in keinem Fall auf den Web-Seiten erscheinen dürfen (und auf die auch nicht in der o.g. Darstellungsweise verlinkt werden darf), kann § 8 Absatz 1 Mediendienste-Staatsvertrag herangezogen werden. Danach sind Inhalte gesetzeswidrig, wenn sie

**gesetzeswidrige
Inhalte**

- gegen Bestimmungen des Strafgesetzbuches verstoßen,
- den Krieg verherrlichen,
- offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden,
- Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne dass ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt; eine Einwilligung ist unbeachtlich,
- in sonstiger Weise die Menschenwürde verletzen.

Grundsätzlich sind Diensteanbieter gemäß § 8 Abs. 2 TDG nicht verpflichtet, die von ihnen übermittelten oder gespeicherten fremden Informationen zu überwachen

**Überwachungs-
pflicht für Inhalte?**

und aktiv (d. h. gezielt) nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit bzw. rechtswidrige Inhalte hinweisen. Da jedoch vom Bürger an das Web-Angebot von Behörden und Verwaltungen hinsichtlich der Distanz zu rechtswidrigen Inhalten im allgemeinen höhere Maßstäbe angelegt werden, wird an dieser Stelle empfohlen, die Inhalte des Web-Auftritts in Abhängigkeit von Umfang und Aktualisierungsgrad der dort angebotenen Dienste in regelmäßigen Abständen darauf zu überprüfen, ob eigene oder fremde Inhalte rechtswidrig sein könnten. In welchen Zeitabständen eine solche Überprüfung erfolgen sollte, hängt vom Aktualisierungsgrad ab: Werden innerhalb des Angebotes beispielsweise Kommunikationsmöglichkeiten wie Forum oder Chat angeboten, empfiehlt es sich, die Zeitintervalle möglichst kurz zu setzen (ggfls. alle zwei Werktage); bei Angeboten, in denen sich der Inhalt hingegen nicht kontinuierlich ändert, können die Zeitabschnitte der Überprüfung größer gewählt werden (z. B. wöchentlich oder alle zwei Wochen).

Sollte der Anbieter zufällig oder gezielt suchend auf rechtswidrige Inhalte stoßen, ist er trotz des am Anfang dieses Abschnitts genannten Haftungsprivilegs gleichwohl verpflichtet, bei solcher positiver Kenntnis diese Inhalte zu sperren, soweit ihm dies möglich ist.

Sperrungspflicht bei Kenntnis rechtswidriger Inhalte

6.2 Jugendschutz

Exkurs: Neues Jugendschutzgesetz im Gesetzgebungsverfahren

Zum Zeitpunkt der Erstellung dieses Moduls befindet sich das neue Jugendschutzgesetz im Gesetzgebungsverfahren, der Bundestag hat im Juni 2002 den entsprechenden Koalitionsentwurf verabschiedet. Aufgrund dieses noch nicht abgeschlossenen Verfahrens und der damit bestehenden Möglichkeit von Änderungen wird der Gesetzentwurf (JuSchG-E) in diesem Modul noch nicht als Grundlage für Qualitätskriterien herangezogen. Da sich der Entwurf jedoch vom derzeit gelten Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjS) im hier relevanten Bereich der Teledienste nicht so sehr inhaltlich, sondern im wesentlichen darin vom GjS unterscheidet, dass nach dem Gesetzesentwurf nun auch sog. Träger- und Telemedien in die Liste jugendgefährdender Medien aufgenommen werden sollen, kann inhaltlich auf die zur Zeit bestehende Rechtslage verwiesen werden.

Abschnitt 6.2 Aufwand 1, Bedeutung 3

Telemedien werden danach in diese Liste jugendgefährdender Medien aufgenommen, wenn sie unsittlich oder verrohend sind oder zu Gewalttätigkeit, Verbrechen oder Rassenhass anheizen. Die in die Liste aufgenommenen Medien unterliegen anschließend dem sog. Verbreitungsgebot (vgl. § 3 GjS bzw. § 15 JuSchG-E), d. h. sie dürfen Kindern und Jugendlichen weder zugänglich gemacht werden noch in einer Weise vorgehalten werden, die Kindern und Jugendlichen den Zugang hierzu ermöglicht. Den Ländern bleibt es durch Schaffung eines Staatsvertrags überlassen, weiterführende Regelungen zum materiellen Jugendschutz zu schaffen.

Verbreitungsverbot für jugendgefährdende Medien

Für Behörden als Anbieter von Telediensten ist der Bereich Jugendschutz im Gesamtzusammenhang zu beachten: Das zur Verantwortlichkeit für rechtswidrige Inhalte Gesagte (s. 6.1) kann insoweit auf den Jugendschutz-Bereich übertragen

werden, als dass dieser spezielle Bereich der Rechtmäßigkeit mit in die Überprüfung des Web-Angebots bzw. der dort platzierten Links mit einbezogen werden sollte. Eine wirksame Kontrolle in diesem Rahmen setzt dementsprechend voraus, dass der Verantwortliche zumindest die wesentlichen einschlägigen Bestimmungen kennt.

Abschließend ist zu empfehlen, entweder im Impressum oder innerhalb sonstiger Angaben zur Verantwortlichkeit den Hinweis aufzunehmen, dass die Behörde als Diensteanbieter die geltenden Jugendschutzbestimmungen beachtet. Ergänzend kann die Adresse der FSM (Freiwillige Selbstkontrolle der Multimedia-Diensteanbieter, www.fsm.de) mit aufgenommen werden. Dieser zentralen Stelle können Verstöße in diesem Bereich mitgeteilt werden.

7 Mustertexte

Zu 4.2: Erklärung der Behörde zur IT-Sicherheit

Erläuterungen zur Datensicherheit

Sehr geehrter Nutzer, sehr geehrte Nutzerin unseres behördlichen Internet-Service-Angebots!

Da trotz der mittlerweile großen Verbreitung des Internets das Thema Sicherheit noch immer das „heiße Eisen“ dieses Mediums ist und für viele die Unsicherheit bzw. das fehlende Wissen darüber nach wie vor ein Hemmnis für die Nutzung dieses weltweiten Netzwerkes darstellt, möchten wir Ihnen nachstehend einige Informationen sowohl über unsere Sicherheitsvorkehrungen, als auch über Möglichkeiten geben, wie Sie Ihre Sicherheit gegenüber dem Internet erhöhen können.

Wir haben alle erdenklichen Anstrengungen unternommen, um die Sicherheit ihrer Daten sowohl bei der Kommunikation mit uns über das Internet, als auch bei der Verarbeitung in unserer Behörde zu gewährleisten. Um dieses Ziel zu erreichen haben wir eine Vielzahl von Maßnahmen zur Steigerung des Sicherheitsniveaus umgesetzt. Die ständige Anpassung an neue Gefahren und Risiken stellt eine Herausforderung dar, der wir mit unserem Sicherheitsmanagement begegnen. Die in diesem Bereich beschäftigten Mitarbeiter genießen das uneingeschränkte Vertrauen und die Unterstützung der Behördenleitung bei der Wahrnehmung ihrer auf Dauer angelegten Aufgabe. Wir geben uns Mühe, soweit wie möglich durch die Etablierung von Sicherheitsmaßnahmen keine zusätzlichen Erschwernisse für die Nutzer unserer Inhalte zu schaffen. Falls es sich im Einzelfall nicht vermeiden lässt, bitten wir um ihr Verständnis. Falls trotz aller unserer Anstrengungen Fragen oder Vorbehalte ihrerseits offen bleiben haben wir zu den nun folgenden Erklärungen Ansprechpartner benannt, die eine Klärung zu Ihrem Nutzen herbeiführen können.

Wir hoffen, dass wir mit diesen Informationen Ihr Vertrauen in unser Internet-Service-Angebot stärken können.

Verschlüsselung

[Nachfolgender Text muss entsprechend den tatsächlichen Verhältnissen angepasst werden, s.auch den Hinweis zur Verschlüsselung in der Datenschutzerklärung]:

Sobald Sie auf unseren Internet-Seiten personenbezogene Daten eingeben, um diese an uns zu übermitteln, setzen wir für diese Übermittlung eine Verschlüsselung ein. Zur Verschlüsselung wird das Verfahren..... mit einer Schlüssellänge vonbit eingesetzt. Durch diese Verschlüsselung wird erreicht, dass die Datenübermittlung zwischen Ihnen und uns vertraulich erfolgt, also kein Dritter, der den Schlüssel nicht besitzt, die übertragenen Daten lesen oder verändern kann. Die Verschlüsselung wird immer dann eingesetzt, wenn sie zum Schutz ihrer Daten notwendig ist. Sie werden interaktiv darauf aufmerksam gemacht, wenn eine sichere Verbindung durch Verschlüsselung aufgebaut wird. Wir benutzen zur Verschlüsselung Zertifikate des Trustcenters xy. Dieses Trustcenter wurde sorgfältig ausgewählt, um den Sicherheitsbedürfnissen unserer Nutzer gerecht zu

werden. Nähere Ausführungen und Erläuterungen zur Verschlüsselung und geeignete Hilfestellungen erhalten Sie bei den jeweiligen Inhaltsangeboten oder direkt unter folgender Internetadresse: www.behördenname.de/service/verschlueselung

[optional:]

Auch die Kommunikation per E-Mail kann zu Ihrem Nutzen unter Einsatz eines Verschlüsselungsverfahrens erfolgen. Um dieses Verschlüsselungsverfahren nutzen zu können, benötigen Sie ein geeignetes Browser-Plug-In und ein Zertifikat, mit dessen Hilfe Sie ihre Daten verschlüsseln können. In unserer Behörde wird das Browser-Plug-In xy eingesetzt. Weitere Informationen wie Sie dieses oder ein ähnliches Produkt erhalten und bedienen können erhalten sie hier: www.xy.de. Sie können verschlüsselte E-Mails, die dem xy-Standard entsprechen, an jede veröffentlichte E-Mail-Adresse in unserer Behörde senden. Nähere Einzelheiten, insbesondere wie der Austausch privater und öffentlicher Schlüssel erfolgt, haben wir für Sie hier zusammengefasst: www.behördenname.de/service/signatur. Von uns versendete E-Mails bzw. E-Mail-Attachments werden sorgfältig auf Viren oder sonstige Schadfunktionen überprüft. Daher ist es grundsätzlich nicht möglich, dass Ihnen durch versendete Inhalte eine Gefahr entsteht.

Zur Sicherheit unseres Web-Servers

Wir bemühen uns, durch geeignete Maßnahmen unsere „Web-Services“ 365 Tage im Jahr rund um die Uhr verfügbar zu halten, damit Sie von überall auf der Welt zu jeder Uhrzeit unsere Angebote nutzen können. So können Sie sich einen Besuch in unserer Behörde oder zeitraubende Telefonate ersparen und bequem von zu Hause Ihren Anliegen nachgehen. Durch die ständige Verfügbarkeit der Server ist somit ein beiderseitiger Nutzen gegeben. Aus verständlichen Gründen können und möchten wir Ihnen an dieser Stelle keine konkreten Informationen zur Absicherung unseres bzw. unserer Web-Server geben. Doch ohne auf Einzelheiten einzugehen, können wir Ihnen mitteilen, dass unser Internet-Angebot ständig entsprechend dem neuesten Stand der Technik abgesichert wird. Diese Absicherung beinhaltet jeweils aktuell konfigurierte Firewalls, eine kontinuierliche Qualitätssicherung durch von uns in Auftrag gegebene Internet-Attacken (friendly attacks) sowie den Einsatz aktueller Virensoftware. „Echte“ Angriffe aus dem Internet auf unsere Web-Server werden zu Ihrer und unserer Sicherheit ausgewertet und verfolgt.

Im Jahre 200x hat es xx echte Angriffe auf unsere Web-Server gegeben, die alle erfolgreich abgewehrt wurden.

[optional:]

IT-Grundschutz-Zertifikat

Um unsere Bemühungen um die Datensicherheit auch gegenüber Ihnen als Nutzern nachweisen zu können, haben wir unsere Datenverarbeitungssysteme entsprechend den Anforderungen des IT-Grundschutzhandbuchs auditieren lassen. Wir sind dafür mit dem IT-Grundschutz-Zertifikat ausgezeichnet worden. Nähere Informationen hierzu finden Sie unter <http://www.bsi.de/gshb/zert/allge.htm>.

Was Sie selbst für Ihre Sicherheit tun können:

Auch Sie als Nutzer können durch einfache Maßnahmen Vorkehrungen treffen, um Ihre Daten vor Verlust oder ungewolltem Zugriff durch Dritte zu schützen. Schon durch einige wenige Einstellungen in Ihrem Browser können Sie denjenigen, die es auf Ihre Daten abgesehen haben, das Leben schwer machen:

Ausführung aktiver Inhalte verhindern bzw. beschränken:

[optional]:

- Die Nutzung unseres Internet-Angebots ist möglich, ohne dass Sie aktive Inhalte akzeptieren müssen *[optional: ggfls. werden bestimmte Seiten in diesem Fall nicht optimal angezeigt]*. Wenn Sie die Ausführung aktiver Inhalte und damit die Möglichkeit, unbemerkt auf Ihrem Computer schädliche Programme auszuführen, verhindern wollen, deaktivieren Sie die aktiven Inhalte in Ihrem Browser. Informationen hierzu entnehmen Sie bitte dem Hilfe-Menü Ihres Browsers.
- Für die Nutzung unseres Internet-Angebots ist lediglich [1] java, [2] javascript*[optional zu wählen]* erforderlich. Sie können Ihren Browser so einstellen, dass die Ausführung sonstiger aktiver Inhalte verhindert wird. Die Aktivierung von Active X in Ihrem Browser ist zur Nutzung unserer Angebote nicht notwendig. Aus Gründen der IT-Sicherheit raten wir aus heutiger Sicht grundsätzlich von der Aktivierung von Active X im Browser ab.
- Für die Nutzung unseres Internet-Angebots benötigen Sie das Plug-In XYZ. Wir möchten Sie darauf hinweisen, dass die Ausführung aktiver Inhalte (ein Plug-In ist ein Zusatzprogramm zum Browser, welches aktive Inhalte ausführt) dazu führen kann, dass unbemerkt Programme auf Ihrem Computer ausgeführt werden, die u. U. zur Schädigung oder zum Verlust von Dateien führen können. Die Nutzung der von uns bereitgestellten Inhalte mit dem Plug-In XYZ bedeutet für Sie kein Sicherheitsrisiko. Wir testen unsere Inhalte regelmäßig auf schadhafte Funktionen und mögliche Betriebsstörungen.

Technischer Ansprechpartner:

Für alle Fragen rund um das Thema Internet-Sicherheit wenden Sie sich bitte an unsere/n Ansprechpartner/in Herr/Frau..... unter der E-Mail-Adresse ansprechpartner@behoerdenname.de *[optional: an den Datenschutzbeauftragten]*

Zu 5.1.1.: Anbieter- bzw. Behördenkennzeichnung (IMPRESSUM)

Impressum

[Mindest-Inhalt]

Behörde XYZ

Straße

PLZ, Ort

Telefon:

Fax:

E-Mail-Adresse:

Die Behörde XYZ ist eine*[hier bitte die Rechtsform angeben]*. Sie wird vertreten durch den/die *[hier bitte die Vertretungsbezeichnung angeben]*, Herrn/ Frau

Umsatzsteueridentifikationsnummer nach § 27a UStG (soweit vorhanden):

DE

[Empfehlung für erweiterten Inhalt:]

Redaktion der Web-Seiten:

(Name, Anschrift und E-Mail-Adresse des entsprechenden Referats)

Technische bzw. gestalterische Umsetzung:

(Name, Anschrift und E-Mail-Adresse der Web-Agentur bzw. des für die Umsetzung des Inhalts Verantwortlichen)

[weiterer möglicher Inhalt (ggfls. auf zusätzlichen Seiten darzustellen:)]

- Darstellung des Organisationsaufbaus
- Anfahrtsskizze

Zu 5.1.1.: Haftungsausschluss (Disclaimer) - (erweitertes) Impressum

Hinweis zur Verantwortlichkeit für Inhalte:

Das Web-Angebot der Behörde XYZ enthält Links (Weiterleitungen) zu anderen Internetangeboten. Externe Links, also Links zu Internetangeboten dritter Informationsanbieter, sind als solche dadurch gekennzeichnet, dass [1] bei Zeigen des Links mit der Maus die entsprechende Ziel-URL in Ihrer Browser-Adressleiste angezeigt wird/ [2] bei Zeigen des Links mit der Maus ein Quick-Info (hellgelbes Hinweissfähnchen) mit der Ziel-URL erscheint . Die Behörde XYZ ist für den Inhalt von Web-Seiten, die mittels einer solchen Verbindung erreicht werden, nicht verantwortlich. Die auf den gelinkten Seiten wiedergegebenen Meinungsäußerungen und/oder Tatsachenbehauptungen liegen in der alleinigen Verantwortung der jeweiligen Autorin oder des jeweiligen Autors und spiegeln nicht die Meinung der Behörde XYZ wider.

Zu 5.1.1.: Hinweise zum Urheberrecht - (erweitertes) Impressum

Hinweise zu Urheberrechten:

Die Behörde XYZ ist bemüht, in allen Publikationen die Urheberrechte der verwendeten Texte oder Grafiken zu beachten, von ihr selbst erstellte Texte oder Grafiken zu nutzen oder auf lizenzfreies Material zurückzugreifen.

Sämtlicher Inhalt der Web-Seiten der Behörde XYZ ist urheberrechtlich geschützt. Vervielfältigungen und sonstige Verwertungen von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen oder Bildmaterial bedürfen, soweit nicht anders vermerkt, der vorherigen Zustimmung des Urhebers. Alle im Web-Angebot der Behörde XYZ genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen im übrigen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts.

Die Nutzung sämtlicher Informationen oder Daten und das sonstige mit den Daten zusammenhängende Tun, Dulden oder Unterlassen unterliegt ausschließlich deutschem Recht.

Zu 5.1.2. Datenschutzerklärung

Datenschutzerklärung/ Privacy Policy

Sehr geehrter Nutzer, sehr geehrte Nutzerin unseres behördlichen Internet-Service-Angebotes!

Da uns der Schutz Ihrer Privatsphäre sehr wichtig ist, haben wir unser Internet-Angebot so gestaltet, dass dessen Nutzung grundsätzlich anonym möglich ist, d. h. die Zugriffe auf unseren Web-Server werden ohne vollständige Erhebung der IP-Adresse protokolliert.

Nicht personenbezogen werden folgende Nutzungsdaten (automatisch) erhoben:

- die vorherige Seite (URL), von der aus die Datei angefordert wurde
- der Name der Datei,
- das Datum und die Uhrzeit der Abfrage,
- die übertragene Datenmenge,
- der Zugriffsstatus (Datei übertragen, Datei nicht gefunden etc.),
- eine Beschreibung des Typs des verwendeten Webbrowsers.

[welche Daten hier konkret erhoben werden, hängt vom Einzelfall ab: die Auflistung muss also entsprechend angepasst werden]

Die o. g. Daten werden von uns ausschließlich zu statistischen Zwecken ausgewertet. Die Auswertung der Daten erfolgt in anonymer Form, d. h. personenbezogene Nutzerprofile können und werden hierdurch nicht erzeugt. Die Nutzungsdaten werden anschließend gelöscht.

Verwaltungsdaten

Um Ihnen die Nutzung einzelner Services zu ermöglichen, kann es erforderlich sein, dass wir Sie um die Angabe personenbezogener Daten bitten. Hierbei handelt es sich in der Regel um Ihren Namen und Ihre Adresse sowie Ihre E-Mail-Adresse, in einigen Fällen auch um weitere Angaben, die wir für die Bearbeitung des konkreten Verwaltungsvorgangs benötigen.

Soweit solche personenbezogenen Daten auf unseren Web-Seiten bzw. in den jeweiligen Formular-Feldern erhoben werden, bleibt es Ihnen überlassen, ob Sie unseren Service nutzen möchten, die Angabe der Daten erfolgt freiwillig. In jedem Fall erfolgt die Erhebung und Verarbeitung dieser Daten aber ausschließlich zum Zweck der Bearbeitung des konkreten Verwaltungsvorgangs. Eine Weitergabe oder Übermittlung an Dritte oder zu sonstigen Zwecken, etwa Werbung oder Marktforschung, erfolgt nicht.

Ihre personenbezogenen Daten werden verschlüsselt an uns übermittelt und sind somit sicher vor dem unberechtigten Zugriff oder der Veränderung durch Unbefugte. Zur Verschlüsselung verwenden wir..... *(Beschreibung des Verschlüsselungsverfahrens und ggf. der Schlüssellänge)*, erkennbar ist dies in der jeweiligen URL-Zeile durch den Zusatz https:.

Cookies

Cookies sind kleine Textdateien, die beim Besuch von Internet-Seiten (meist unbemerkt) auf Ihrer Festplatte gespeichert werden. Sie dienen dazu, die Nutzung von Internet-Angeboten bedienerfreundlicher zu machen, indem Sie u.a. die Wiedererkennung als Nutzer ermöglichen oder die Web-Seiten entsprechend Ihren vorherigen Besuchen anpassen.

[Mögliche Varianten:]

- Bei der Bereitstellung unseres Internet-Angebotes werden keine Cookies verwendet.
- Bei der Nutzung unseres Internet-Angebotes wird ein sog. Session-Cookie verwendet. Dies ist eine kleine Textdatei, die nur während der tatsächlichen Nutzung unseres Internet-Angebotes und auch nur im Arbeitsspeicher Ihres Systems gespeichert und nach Beendigung, d. h. nach Verlassen der Seiten von Ihrem Browser automatisch gelöscht wird. Das Session-Cookie dient dazu.....*[hier den konkreten Zweck des Session-Cookies nennen, z. B. Authentifizierung des Nutzers gegenüber geschützten Bereichen]*
- Bei der Nutzung unseres Internet-Angebotes wird ein dauerhaftes Cookie verwendet. Dies ist eine kleine Textdatei, die auf Ihrer Festplatte über einen Zeitraum von x Monaten/Jahren gespeichert wird. Das Cookie dient dazu.....*[hier den konkreten Zweck des dauerhaften Cookies nennen, z. B. Erstellung von Nutzerprofilen etc.]*

Zusätzlich bei der zweiten und dritten Option: Die Nutzung unserer Web-Seiten ist auch ohne Cookies möglich. Wenn Sie keine Cookies akzeptieren möchten, müssen Sie Ihren Browser entsprechend konfigurieren. Informationen hierzu finden Sie im jeweiligen Hilfe-Menü Ihres Browsers.

Ihre Rechte als Nutzer („Betroffener“)

Nach den §§ 19 - 20 des Bundesdatenschutzgesetzes bzw. den entsprechenden Vorschriften des Datenschutzgesetzes *[hier bitte ggfls. den Namen des einschlägigen Landesdatenschutzgesetzes eintragen]* stehen Ihnen als Nutzer (das Gesetz spricht hier von „Betroffener“) bestimmte Rechte zu, die Sie gegenüber der Daten verarbeitenden Stelle geltend machen können. Diese Rechte sind

- das Auskunftsrecht, wonach Sie jederzeit unentgeltlich Auskunft über die über Sie gespeicherten Daten verlangen können,
- das Benachrichtigungsrecht, welches die Daten verarbeitende Stelle dazu verpflichtet, Sie darüber zu benachrichtigen, wenn Daten über Sie ohne Ihre Kenntnis erhoben werden
- das Berichtigungsrecht, wonach Sie jederzeit veranlassen können, unrichtig erhobene oder gespeicherte Daten berichtigen zu lassen,
- das Löschungs- bzw. Sperrungsrecht, wonach Sie Daten, die unzulässiger Weise erhoben oder deren Speicherung nicht mehr erforderlich ist, löschen bzw. sperren lassen können und

- das Widerspruchsrecht, wonach Sie der Nutzung der Daten widersprechen können, wenn Sie ein besonderes, schutzwürdiges Interesse glaubhaft machen können.

Wir möchten, dass Sie diese Rechte bei Bedarf möglichst einfach und unkompliziert wahrnehmen können. *[Optional]*: [1] Aus diesem Grunde haben wir für Sie ein Formular bereitgestellt, welches Sie nur auszufüllen und uns zuzusenden brauchen. Sie erhalten dann umgehend Antwort. [2] Wenden Sie sich daher einfach per E-Mail an den Datenschutzbeauftragten (s. u.), Sie erhalten dann umgehend Antwort.

Datenschutzbeauftragter

Für weitere Fragen rund um das Thema Datenschutz wenden Sie sich bitte an unsere/n Datenschutzbeauftragte/n, Herrn/Frauunter der E-Mail-Adresse datenschutzbeauftragter@behoerdenname.de. Er/Sie ist auch Ansprechpartner für die Durchsetzung Ihrer Rechte als Betroffener.

8 Checklisten

Die nachfolgende Checkliste erlaubt es, einen schnellen Überblick zu erhalten, an welchen Stellen der eigene Web-Auftritt nachgebessert werden sollte. Alle Fragen sind so gestellt, dass die Antwort „ja“ bedeutet „so ist’s gut“ und die Antwort „nein“ „hier ist noch Handlungsbedarf“. Manche Fragen sind für einen Internet-Auftritt nicht relevant und können demzufolge ignoriert werden.

8.1 Zugang (s. Kap. 2)

8.1.1 (Technische) Zugänglichkeit/ Auffindbarkeit (s. Kap. 2.1)

8.1.1.1 Auffindbarkeit im Internet (s. Kap. 2.1.1)

- Findet man die Behörde oder die Dienstleistung unter den ersten 20 Treffern von Suchmaschinen? ja nein
- Findet man die Behörde oder die Dienstleistung über ein einschlägiges Portal, z. B. www.bund.de? ja nein
- Ist die gewählte URL kurz und prägnant? ja nein
- Sind „Verschreibungs-URLs“ belegt? ja nein

8.1.1.2 Kompatibilität (s. Kap. 2.1.2)

- Kann jeder Bürger den Web-Inhalt nutzen, ohne Anpassungen an den Einstellungen (Default) seines Web-Browser vorzunehmen (aktive Inhalte, Java-Applets, Frames, Cookies, Firewall, Werbeblocker)? Falls dies nicht der Fall ist, existiert zumindest eine alternative Variante (z. B. eine Nur-Text-Version)? Falls dies nicht der Fall ist, erhält er zumindest entsprechende Anpassungshinweise und Hilfestellungen oder bleibt der Bildschirm leer? ja nein
- Kann das Internetangebot auch mit einem textbasierten Browser benutzt werden bzw. mit einem Browser, dessen Grafikfunktion deaktiviert ist? ja nein
- Wenn das Angebot mit Frames gestaltet ist, existiert auch eine framelose Variante? ja nein
- Sind Inhalte ohne die Installation von spezifischer Betrachtungssoftware (Plug-Ins) erreichbar? Wenn nicht, existieren auch andere plattform- und browserunabhängige Zugänge? ja nein

- Ist die Bildschirmdarstellung mit allen gängigen Browsern optimal? Falls nein, wird eindeutig darauf hingewiesen, für welchen Browser oder welche Bildschirmauflösungen die Darstellung optimiert ist? ja nein
- Ist das Angebot mit älteren oder „exotischen“ Browsern nutzbar? ja nein

8.1.1.3 Performanz (s. Kap. 2.1.3)

- Werden bei der Startseite aktuelle Richtwerte bzgl. Ladezeit (höchstens acht Sekunden) und Dateigröße (maximal 60 bis 70 KB pro Seite) eingehalten? ja nein
- Falls eine grafikintensive Version für Bürger mit schneller Anbindung an das Internet existiert: Gibt es alternativ eine Light-Version für die Bürger mit langsamen Internetzugängen? ja nein
- Werden Grafiken durch alternative Texte beschrieben? ja nein
- Werden große Grafikdateien (> 50 k) zuerst in einer Mini-Vorschau („thumbnails“) angezeigt? ja nein
- Wird die subjektiv empfundene Wartezeit durch Mechanismen wie z. B. die nacheinander erfolgende Darstellung von Text und Grafik und das Laden von Grafiken in einer Grobansicht verkürzt? ja nein

8.2 (Inhaltliche) Erschließung (s. Kap. 2.2)

8.2.1 Allgemeine Orientierung (s. Kap. 2.2.1)

- Wenn die Verwaltungsseiten Teil eines umfassenden Angebots sind: Ist das Verwaltungsangebot auf der Startseite/ dem Navigationsframe zu finden? ja nein
- Wird die Auffindbarkeit von Inhalten durch geeignete Hilfsmittel wie z. B. Inhaltsverzeichnisse, alphabetische Verzeichnisse von Verwaltungsstellen und Dienstleistungen, Sitemaps und einen vollständigen Index gewährleistet? ja nein
- Ist das Angebot verständlich strukturiert? ja nein
- Werden Einstiegsmöglichkeiten für best. Zielgruppen (Bürger, Behörden, Wirtschaft, Kooperationspartner) angeboten? ja nein
- Werden zur Navigation an Lebenssituationen (Lebenslagenprinzip) orientierte Menüpunkte angeboten? ja nein

- Kann man auf einen Blick erkennen, dass es sich bei dem Anbieter um eine Behörde handelt? ja nein
- Werden externe Links deutlich gekennzeichnet? ja nein

8.2.1.1 Suchmaschine (s. Kap. 2.2.2)

- Wird eine Volltextsuche angeboten? ja nein
- Wird zusätzlich eine Stich- und Schlagwortsuche angeboten? ja nein
- Ist die Suche fehlertolerant? Werden z. B. Unterschiede zwischen Singular und Plural oder „Verschreibungen“ toleriert? ja nein
- Ist die das Antwort-Zeitverhalten der Suchmaschine akzeptabel und die Präsentation des Suchergebnisses (Art und Umfang des Suchergebnisses wie z. B. die Skalierbarkeit der Trefferliste (max. Treffer = 10/ 20/ 30 etc.)) einstellbar? ja nein
- Existiert eine erweiterte Suche mit Und-/ Oder-/ Nicht-Verknüpfungen? ja nein
- Wird ein Ranking im Ergebnis angezeigt? ja nein
- Ist die Bedienung der Suchmaschine einfach, verständlich und an den unterschiedlichen Kenntnisstand der Bürger anpassbar? ja nein
- Werden bei nicht gefundenen Suchbegriffen der Suchmaschine Hilfen für eine weitere Suche angeboten bzw. bei zu viel gefundenen Begriffen erläutert, wie die Suche einzuschränken ist? ja nein

8.2.1.2 Mehrsprachigkeit (s. Kap. 2.2.3)

- Ist das Angebot mehrsprachig gestaltet? ja nein
- Wird dem fremdsprachigen Publikum verdeutlicht, dass es evtl. nur eine reduzierte Teilmenge des Gesamtgebots in seiner Sprache erhält? ja nein

8.2.1.3 Barrierefreiheit (s. Kap. 2.2.4)

- Ist vorstellbar, dass der Dialog so angepasst werden kann, dass Behinderte das System nutzen können? ja nein
- Sind integrierte Funktionen zum Support einer spezifischen barrierefreien Darstellung vorhanden? ja nein

- Können die Informationen von Bürgern aufgenommen werden, die nicht hören oder sehen können? ja nein
- Ist die Anwendung z. B. auch ohne Maus (komplett über die Tastatur) bedienbar? ja nein
- Können assistive Tools wie z. B. Screenreader genutzt werden? ja nein

8.2.1.4 Navigation (s. Kap. 2.2.5)

- Wird im Titel des Browsers immer der Titel der aktuell aufgerufenen Seite angezeigt, sodass man sie bookmarken kann? ja nein
- Ist in den linear strukturierten Teilbereichen des Angebots ein Navigieren mit den Tasten „vorherige Seite“ und „nächste Seite“ möglich? ja nein
- Kann der Bürger bei der Bearbeitung von Web-Formularen mit der üblichen Browser-Navigation ein oder mehrere Fenster zurück navigieren? ja nein
- Existiert ein Logbuch der Aktionen bzw. erfüllt die History-Funktion des Browsers diesen Zweck, sodass immer mehrere Arbeitsschritte rückgängig gemacht werden können? ja nein
- Weiß der Bürger zu jedem Zeitpunkt, an welcher Stelle im Angebot er sich befindet und was er hier tun kann? ja nein
- Können zu jedem Zeitpunkt die Kernbereiche des Angebots angewählt werden (Startseite, Index, Inhaltsverzeichnis, vorige und nächste Seite, Ober- bzw. Unterkategorie)? ja nein
- Ist die Anzahl der notwendigen 'Klicks' bis zum Dienstleistungsangebot niedrig gehalten? ja nein
- Werden 'Sackgassen' ohne Links (dead end page) vermieden? ja nein
- Werden 'tote' Links vermieden? ja nein

8.2.1.5 Hilfen (s. Kap. 2.2.6)

- Sind evtl. auftretende Fehlermeldungen klar, verständlich und hilfreich? ja nein
- Besteht die Möglichkeit, persönlichen Support (User-Help-Desk, Call-Center/ Hotline) in Anspruch zu nehmen? ja nein
- Wird eine FAQ angeboten? ja nein
- Erhält der Bürger ausreichende Informationen, Hilfestellung, Bezugshinweise, falls zusätzliche Hard- oder Software ja nein

für die Nutzung von Online-Dienstleistungen (z. B. qualifizierte elektronische Signatur) notwendig sind?

- Werden kontextsensitive Hilfen angeboten? ja nein
- Sind Erläuterungen zur Bedienung der Internetseiten vorhanden? ja nein
- Sind Informationen zur (technischen) Ausführung der Dienstleistung vorhanden? ja nein
- Existiert eine Hilfe zu inhaltlichen und funktionalen Bearbeitungsfragen, die jederzeit aufgerufen werden kann? ja nein
- Werden Online-Hilfen bei komplizierten Formularen angeboten? ja nein

8.3 Inhaltliche Angebote und Funktionen (s. Kap. 3)

8.3.1 Informationsangebote (s. Kap. 3.1)

8.3.1.1 Umfang und Tiefe (s. Kap. 3.1.1)

8.3.1.1.1 Orientierungsinformationen (s. Kap. 3.1.1.1)

- Werden aus allen relevanten Einrichtungen und Verwaltungsbereichen grundlegende Informationen wie Adresse, Telefonnummer, Öffnungszeiten, Ansprechpartner und Zuständigkeiten angeboten? ja nein
- Erhält der Bürger Informationen zur Erreichbarkeit (wie Erreichbarkeit mit öffentlichen Verkehrsmitteln, Standortanzeige auf dem Stadt- und Gebäudeplan)? ja nein
- Kann der Bürger vorgesetzte und nachgeordnete Behörden einfach finden? ja nein

8.3.1.1.2 Informationen zu Verwaltungsaufgaben und –leistungen (s. Kap. 3.1.1.2)

- Sind aus allen relevanten Einrichtungen und Verwaltungsbereichen Informationen zu den angebotenen Dienstleistungen verfügbar? ja nein
- Gibt es detaillierte Anspruchsinformationen? ja nein
- Werden Informationen über die Verwaltungsorganisation/ -aufgabe und -struktur angeboten? ja nein

- Werden Basisinformationen über aktuelle Planungen (z. B. Stadtplanung in Kommunen) und Entwicklungen (Gesetzesvorhaben in Städten und Ländern) angeboten? ja nein
- Werden zu bestimmten ausgesuchten Themen weiterführende Informationen (z. B. Ablauf von Planungen und Gesetzgebungsverfahren) als Downloads oder über Links zugänglich gemacht? ja nein
- Sind einschlägige gesetzliche Vorschriften aufrufbar? ja nein

8.3.1.2 Anforderung von Informationsmaterial (s. Kap. 3.1.2)

- Ist es möglich, sich Informationsmaterial (z. B. Merkblätter) online abzurufen oder auf dem Postweg zuschicken zu lassen? ja nein
- Ist der Download von Broschüren etc. möglich? ja nein
- Sind die zum Download angebotenen Informationen in einem plattformübergreifenden Format (z. B. PDF, Postscript, ASCII etc.) verfügbar? ja nein

8.3.1.3 Nutzungsqualität (s. Kap. 3.1.3)

8.3.1.3.1 Verständlichkeit (s. Kap. 3.1.3.1)

- Gibt es für notwendige Fachbegriffe eine entsprechende Erläuterung (z. B. Fußnote, Glossar)? ja nein
- Werden nicht zum Thema der besuchten Seite gehörende Fachbegriffe vermieden? ja nein
- Ist die verwendete Sprache verständlich, am Alltag orientiert und entspricht sie dem Kundenverständnis (indem Amtssprache vermieden wird)? ja nein
- Wird EDV-Jargon vermieden? ja nein
- Sind die gewählten Begriffe, Bezeichnungen und Symbole in den Überschriften und Gliederungen verständlich und umgangssprachlich angepasst? ja nein
- Werden regionale Eigenheiten, die national und international un- bzw. missverständlich sind, vermieden? ja nein
- Existiert bei langwierigen Prozessen (z. B. einer komplexen DB-Abfrage) eine Prozessfortschrittsanzeige, um dem Bürger Rückmeldungen über den Zustand des Arbeitsablaufs zu geben? ja nein

8.3.1.3.2 Korrektheit und Vertrauenswürdigkeit des Angebots (s. Kap. 3.1.3.2)

- Sind die Verwaltungsseiten in Hinblick auf ihre Korrektheit (Rechtschreibung, Grammatik, Tabellenformatierungen und ungültige Links) überprüft worden? ja nein
- Sind Mitarbeiter für die Pflege der Verwaltungsseiten verantwortlich? ja nein
- Wird in hinreichender Form darüber informiert, wer der inhaltlich Verantwortliche bzw. die inhaltlich verantwortliche Institution des Informationsangebots ist? ja nein

8.3.1.3.3 Aktualität (s. Kap. 3.1.3.3)

- Sind die eingestellten Informationen und Kontakte der Behörde aktuell? ja nein
- Sind die Beiträge mit Aktualitätshinweisen versehen und somit als aktuelle oder neue Inhalte kenntlich gemacht? ja nein
- Existiert ein Newsticker für häufig wechselnde und neue hervorzuhebende Informationen/ Mitteilungen? ja nein

8.3.2 Kommunikationsangebote (s. Kap. 3.2)

8.3.2.1 E-Mail (s. Kap. 3.2.1)

8.3.2.1.1 Umfang und Tiefe (s. Kap. 3.2.1.1)

- Besteht eine zentrale Kontakt- bzw. Beschwerdemöglichkeit (E-Mail und Telefonnummer)? ja nein
- Besteht die Möglichkeit, einzelne Organisationseinheiten gezielt per E-Mail zu erreichen? ja nein
- Besteht die Möglichkeit, die für bestimmte Aufgaben zuständigen Sachbearbeiter gezielt per E-Mail zu erreichen? ja nein
- Bestehen Vertretungsregelungen für die Bearbeitung eingehender E-Mails? ja nein
- Kann man jederzeit per E-Mail zu den inhaltlich Verantwortlichen des WWW-Angebots Kontakt aufnehmen? ja nein

8.3.2.1.2 Nutzungsqualität (s. Kap. 3.2.1.2)

- Ist ein bestimmtes Antwortverhalten der Verwaltung geregelt und dem Bürger gegenüber garantiert (z. B. eine Ant-

wort innerhalb von zwei Werktagen)?

8.3.2.2 Newsletter (s. Kap. 3.2.2)

- Besteht die Möglichkeit, einen Newsletter zu abonnieren? ja nein
- Sind die Newsletter themenspezifisch gegliedert? ja nein

8.3.2.3 Mailinglisten (s. Kap. 3.2.3)

- Besteht die Möglichkeit, sich in eine Mailingliste einzutragen? ja nein
- Sind die Mailinglisten themenspezifisch gegliedert? ja nein

8.3.2.4 Diskussionsangebote (s. Kap. 3.2.4)

- Werden den Bürgern neue Möglichkeiten zum Einfluss und zur Mitsprache (durch Umfragen, Petitionen, Chats, Diskussionsforen, Abstimmungen) gegeben? ja nein
- Können Bürger Anregungen (z. B. über ein Online-Formular) geben? ja nein
- Sind diese neuen Kommunikationsmöglichkeiten auch für Gelegenheitsnutzer verständlich? ja nein
- Werden „Schwarze Bretter“ angeboten, die auch die Kommunikation der Bürger untereinander ermöglichen? ja nein
- Kann zu bestimmten Anlässen/ Themen mit der Verwaltung kommuniziert werden (z. B. in einem Diskussionsforum)? ja nein
- Sind angebotene Diskussionsforen gegliedert (z. B. in offene Foren (oberste Ebene wie z. B. "Themenübersicht", aber auch dringende Angelegenheiten und Bekanntmachungen), Wurzelforen (spezifizierte und detaillierte Themen wie beispielsweise "Arbeit") und Zweigforen ("Berufsbildung", "Fortbildung", "Arbeitsbeschaffung", "Arbeit & Gesundheit"))? ja nein
- Werden Diskussionsforen direkt von einem Mitarbeiter erstellt und gewartet (z. B. der Moderator eines Forums)? ja nein
- Sind „Schwarze Bretter“ themenspezifisch (ähnlich den Foren) gegliedert (keine pure Ansammlung von Mitteilungen) gegliedert? ja nein
- Ist sichergestellt, dass die Anregungen und Beiträge (z. B. in Foren) der Bürger bearbeitet und ausgewertet werden? ja nein

- Wird der Bürger über den weiteren Verlauf der Bearbeitung einer Anregung/ eines Diskussionsbeitrags informiert? ja nein
- Ist sichergestellt, dass der Bürger über die Veränderungen/ Folgen seiner Anregungen und Beiträge ein Feedback erhält? ja nein

8.3.2.5 Chat (s. Kap. 3.2.5)

- Besteht die Möglichkeit, einem Chat beizutreten? ja nein

8.3.3 Transaktionsangebote (s. Kap. 3.3)

Exkurs: Elektronische Signaturen (s. Kap. 3.3)

- Werden dem Bürger Informationen über den Einsatz elektronischer Signaturen gegeben? ja nein
- Werden dem Bürger Informationen gegeben, wo er elektronische Signaturen erhalten kann? ja nein
- Können Dokumente mit einer fortgeschrittenen elektronischen Signatur (dies ist in der Regel eine softwarebasierte Signatur) unterschrieben werden, die notwendig ist, um den Autor des Dokuments zweifelsfrei authentisieren zu können? ja nein
- Können Dokumente mit einer qualifizierten elektronischen Signatur (dies ist in der Regel eine hardwarebasierte Signatur) unterschrieben werden, die notwendig ist, wenn Schriftform gefordert wird? ja nein
- Kann der Zeitpunkt der Signierung durch einen elektronischen Zeitstempel dokumentiert werden? ja nein
- Kann der Zeitpunkt des Absendens bzw. der Zustellung durch einen elektronischen Zeitstempel dokumentiert werden? ja nein
- Werden dem Bürger Mechanismen zur Verfügung gestellt, um sich durch Prüfung einer elektronischen Signatur (fortgeschritten bzw. qualifiziert) von der Authentizität der heruntergeladenen Dokumente überzeugen zu können? ja nein
- Werden dem Bürger Mechanismen zur Verfügung gestellt, um sich durch Zertifikatsprüfung von der Gültigkeit und Authentizität des Zertifikats überzeugen zu können? ja nein
- Existiert eine neutrale Stelle mit Notariatsfunktion (Intermediär), die für den Bürger die Signatur- und Zertifikatsprüfung durchführen und das Ergebnis der Prüfung weiterleiten? ja nein

könnte?

- Existiert eine neutrale Stelle mit Notariatsfunktion (Intermediär), die die Übertragung der Dokumente einschließlich Absende- und Zustelldatum zweifelsfrei dokumentiert und bei Bedarf quittieren könnte? ja nein
- Können die übertragenen Daten so verschlüsselt werden, dass die neutrale Stelle mit Notariatsfunktion die Daten nicht mitlesen kann? ja nein
- Ist die neutrale Stelle mit Notariatsfunktion außerhalb der Verwaltung angesiedelt? ja nein
- Existieren für den Fall, dass die Notariatsfunktion von der Verwaltung selbst wahrgenommen wird, entsprechende Sicherheitsvorkehrungen, die eine Trennung von Fachanwendung und Notariatsfunktion sicherstellen? ja nein

8.3.3.1 Umfang und Tiefe (s. Kap. 3.3.1)

- Werden aus allen Bereichen gängige Formulare zum Download angeboten, die anschließend ausgedruckt, ausgefüllt und auf dem Postweg versendet werden? ja nein
- Können überschaubare Formulare (bis zu zwei Seiten) am Bildschirm ausgefüllt und im Anschluss daran auf dem Postweg versendet werden? ja nein
- Können am Bildschirm ausfüllbare Formulare elektronisch versendet werden? ja nein
- Werden für komplizierte Vorgänge/ Formulare Ausfüllhilfen mittels strukturierter Dialoge angeboten? ja nein
- Werden Bestätigungen über den erfolgreichen Empfang von E-Mails oder Transaktionsdaten an den Kunden gesendet? ja nein
- Wird die Abfragemöglichkeit des Bearbeitungsstatus (Prozestransparenz durch 'track and trace') einer Transaktion angeboten? ja nein
- Hat der Bürger auch nach Abschluss der Dienstleistungserbringung eine Online-Möglichkeit, um Fragen zu klären? ja nein
- Wird der Bürger bei wichtigen ihn betreffenden Veränderungen (z. B. beim Ablauf von Fristen) mit pro-aktiven Informationen versorgt? ja nein

8.3.3.2 Payment (s. Kap. 3.3.2)

- Besteht eine „echte“ Online-Bezahlungsfunktion? ja nein
- Findet eine Eingabeüberprüfung (z. B. das Überprüfen von vorhandenen BLZ oder der Zahlungsfähigkeit bei Kreditkartenzahlung) statt? ja nein
- Werden unterschiedliche elektronische Bezahlungsfunktionen (Rechnung, Lastschrift, Überweisung, Kreditkarte, E-Cash, eigenes System, externe Anbieter) angeboten? ja nein

8.3.3.3 Nutzungsqualität (s. Kap. 3.3.3)

8.3.3.3.1 Einbindung in das Gesamtangebot (s. Kap. 3.3.3.1)

- Ist das Transaktionsangebot in das Gesamtangebot integriert? ja nein
- Sind die bereitgestellten Formulare und Transaktionsangebote über die zu den betreffenden Geschäftsvorfällen bereitgestellten Informationsseiten direkt aufrufbar? ja nein

8.3.3.3.2 Aufwand (s. Kap. 3.3.3.2)

- Ist der kundenseitige Aufwand und die Komplexität der Bürgerauthentisierung (qualifizierte elektronische Signatur nur wenn nötig) skalierbar? ja nein
- Werden Stammdaten hinterlegt, sodass Mehrfacheingaben unnötig sind? ja nein

8.3.3.3.3 Medienbruchfreiheit (s. Kap. 3.3.3.3)

- Können Anlagen online übermittelt werden? ja nein
- Ist das verwaltungsseitige Ergebnis ebenfalls übermittelbar? ja nein
- Ist eine Kombination zwischen „klassischen“ (Telefon, Fax, Post) und Online-Verfahren möglich, sofern die Transaktion nicht ohne Medienbruch durchführbar ist (z. B. aufgrund von Gesetzesvorschriften)? ja nein

8.3.3.3.4 Plattformunabhängigkeit (s. Kap. 3.3.3.4)

- Sind die Dokumente, die dem Bürger zum Download angeboten werden, durchgängig im PDF-Format angelegt? ja nein
- Werden darüber hinaus auch Dokumente in anderen Formaten angeboten? ja nein

8.3.3.3.5 Handhabung von Formularen (s. Kap. 3.3.3.5)

- Werden Felder in Abhängigkeit von zuvor getätigten Eingaben automatisch vervollständigt? ja nein
- Werden Defaultwerte vorgegeben und entsprechen diese auch der Mehrzahl der Fälle? ja nein
- Werden Ausfüllhilfen (z. B. erläuternde Texte/ Hinweise) bei Formularen angeboten? ja nein
- Finden Eingabeüberprüfungen bezogen auf formale Richtigkeit, Vollständigkeit (zur schnelleren Bearbeitung des Vorgangs und z. B. um Rückfragen zu vermeiden) und Konsistenz statt? ja nein
- Gibt es Verfahren zur Wiederaufnahme der Transaktion nach (unbeabsichtigten) Verbindungsunterbrechungen oder Fehlern? ja nein
- Sind bei ähnlichen Interaktionen resp. Arbeitsaufgaben (z. B. Formularbearbeitung) die Arbeitsschritte und Dialoge ähnlich gestaltet? ja nein

8.4 IT-Sicherheit (s. Kap. 4)

8.4.1 IT-Sicherheitsmanagement⁴⁰ (s. Kap. 4.1)

- Ist das IT-Management als Bestandteil des E-Government dauerhafte Aufgabe der Verwaltungsstruktur? ja nein
- Existiert ein IT-Sicherheitsbeauftragter, dem diese Aufgaben übertragen worden sind? ja nein

8.4.2 Erklärungen der Behörde zur IT-Sicherheit (s. Kap. 4.2)

- Gibt es eine Sicherheitserklärung zu Fragen der Sicherheit des Web-Auftritts (separat oder in die Datenschutzerklärung integriert)? ja nein
- Enthält die Sicherheitserklärung weitere für den Bürger wichtige Sicherheitsinformationen
 - zur Verbindungssicherheit, insbesondere zur Verschlüsselung der Kommunikation zwischen Behörde und Bürger, ja nein

⁴⁰ Die Fragen dieses Abschnitts zielen zum Teil auf die Umsetzung der Maßnahmen des Abschnitts „Sicherer Internet-Auftritt im E-Government“ in Kapitel „IT und IT-Sicherheit“ ab.

- wie die Virenfreiheit des Angebots sichergestellt wird,
- wie die Virenfreiheit von Downloads (Formularen) sichergestellt wird,
- zur Firewall-Technik und Netzwerksicherheit?
- Werden Informationen gegeben, wie sich der Bürger vor allgemeinen Sicherheitsrisiken selbst schützen kann? ja nein
- Sind die Informationen verständlich aufbereitet? ja nein
- Wird ein Ansprechpartner (einschließlich E-Mail-Adresse oder Telefon-Nr.) genannt, an den sich der Bürger bei Fragen zur Sicherheit wenden kann? ja nein

8.4.3 Aktive Inhalte (s. Kap. 4.3)

- Wird im Informationsangebot auf den Einsatz von ActiveX-Komponenten verzichtet? ja nein
- Wird im Informationsangebot auf den Einsatz von Java-Komponenten verzichtet? ja nein
- Wird im Informationsangebot auf den Einsatz von JavaScript-Komponenten verzichtet? ja nein
- Kann das Informationsangebot ohne Verwendung von Plug-Ins dargestellt werden? ja nein

8.4.4 Kryptografie und Authentisierung⁴¹ (s. Kap. 4.4)

- Kann das Informationsangebot – insbesondere Informationen mit sensiblen Daten – über eine verschlüsselte Verbindung genutzt werden? ja nein
- Ist das zur Verschlüsselung und zur Authentisierung verwendete Zertifikat von einem anerkannten Trust-Center ausgestellt worden? ja nein
- Kann die Gültigkeit des Zertifikates schnell und zuverlässig überprüft werden? ja nein
- Können ausschließlich als sicher eingestufte Verfahren für einen Verbindungsaufbau gewählt werden (z. B. TLS oder SSLv3)? ja nein
- Ist eine Mindestlänge für symmetrische Schlüssel festgelegt, die dem aktuellen Sicherheitsstandards entspricht (z. B. ja nein

⁴¹ Die Fragen dieses Abschnitts stellen die Verbindung zu den Maßnahmen des Abschnitts „Kryptografie im E-Government“ in Kapitel IV B „IT und IT-Sicherheit“ her.

128-Bit-RC4)?

- Ist eine Mindestlänge für asymmetrische Schlüssel festgelegt, die dem aktuellen Sicherheitsstandards entspricht (z. B. 1024-Bit-RSA)? ja nein
- Können im Rahmen des Informationsangebots Zertifikate für eine Ende-zu-Ende-Verschlüsselung abgerufen werden? ja nein

8.4.5 Absicherung von Web-Servern per Firewall (s. Kap. 4.5)

- Ist die Verbindung zum Internet – auch wenn sie über ein nicht-öffentliches Netz (z. B. den Informationsverbund Berlin-Bonn (IVBB)) erfolgt – durch einen Paketfilter gesichert? ja nein
- Ist der Paketfilter so konfiguriert, dass zunächst jegliche Kommunikation zwischen dem Internet und dem Web-Server verboten ist und anschließend nur die erforderlichen Verbindungen zugelassen werden? ja nein
- Ist die Verbindung zum Internet – auch wenn sie über ein nicht-öffentliches Netz (z. B. IVBB) erfolgt – durch ein Application Gateway gesichert? ja nein
- Ist das Application Gateway so konfiguriert, dass zunächst jegliche Kommunikation zwischen dem Internet und dem Web-Server verboten ist und anschließend nur die erforderlichen Verbindungen zugelassen werden? ja nein
- Ist das Application Gateway so konfiguriert, das alle Daten einer erlaubten Verbindung zwischen Internet und Web-Server inhaltlich analysiert werden? ja nein
- Ist die Verbindung zum Intranet – auch wenn sie über ein nicht-öffentliches Netz (z. B. IVBB) erfolgt – durch einen Paketfilter gesichert? ja nein
- Ist der Paketfilter so konfiguriert, dass zunächst jegliche Kommunikation zwischen dem Intranet und dem Web-Server verboten ist und anschließend nur die erforderlichen Verbindungen zugelassen werden? ja nein
- Ist die Verbindung zum Intranet – auch wenn sie über ein nicht-öffentliches Netz (z. B. IVBB) erfolgt – durch ein Application Gateway gesichert? ja nein
- Ist das Application Gateway so konfiguriert, dass zunächst jegliche Kommunikation zwischen dem Intranet und dem Web-Server verboten ist und anschließend nur die erforderlichen Verbindungen zugelassen werden? ja nein
- Ist das Application Gateway so konfiguriert, das alle Daten einer erlaubten Verbindung zwischen dem Intranet und dem

Web-Server inhaltlich analysiert werden?

8.4.6 Administration von Web-Servern⁴² (s. Kap. 4.6)

- Sind die Maßnahmen des IT-Grundschutzhandbuchs, insbesondere des Abschnitts über WWW-Server, berücksichtigt worden? ja nein
- Werden die Inhalte des Web-Servers auf einem schreibgeschützten Datenträger gespeichert (z. B. CD-ROM)? ja nein
- Werden die Inhaltsdaten des Web-Servers automatisch mit einem gesicherten Kontrolldatenbestand verglichen (z. B. unter Verwendung eines sog. Watchdog)? ja nein
- Ist sichergestellt, dass Daten nicht vom Internet aus auf den Web-Server geschrieben werden können? ja nein
- Ist sichergestellt, dass Daten nicht vom Intranet aus auf den Web-Server geschrieben werden können? ja nein

8.5 Datenschutz (s. Kap. 5)

8.5.1 Transparenz (s. Kap. 5.1)

8.5.1.1 Anbieter bzw. Behördenkennzeichnung (s. Kap. 5.1.1)

- Wird im Web-Angebot eine Behördenkennzeichnung veröffentlicht? ja nein
- Enthält die Behördenkennzeichnung Namen und Anschrift der Behörde sowie den Behördenleiter? ja nein
- Enthält die Behördenkennzeichnung Angaben über sämtliche Telefon- und Faxnummern sowie zumindest eine zentrale E-Mail-Adresse? ja nein
- Wird ggf. auf eingeschaltete Hosting-Services und sonstige Service-Provider hingewiesen, soweit keine Datenverarbeitung im Auftrag vorliegt? ja nein
- Sind die Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar? ja nein
- Ist die Behördenkennzeichnung direkt von der Leitseite ja nein

⁴² Zur sicheren Administration eines WWW-Servers finden sich ausführliche Informationen im IT-Grundschutzhandbuch des BSI, insbesondere in Kapitel 7.5 WWW-Server.

(Homepage) aus verfügbar (one-click away)?

- Ist der direkte Zugriff auf die Behördenkennzeichnung von allen Seiten aus möglich? ja nein

8.5.1.2 Datenschutzerklärung/ Privacy Policy (s. Kap. 5.1.2)

- Erfolgt eine Unterrichtung des Bürgers über das Ob und Wie der Erhebung, Verarbeitung und Nutzung personenbezogener Daten? ja nein
- Wird in der Unterrichtung eine vollständige Darstellung der Erhebung, Speicherung, Nutzung und Übermittlung der personenbezogenen Daten gegeben, differenziert nach unterschiedlichen Datenarten (Nutzungsdaten, Bestandsdaten etc.)? ja nein
- Wird ggf. auf die Verarbeitung von Daten außerhalb des europäischen Wirtschaftsraums hingewiesen? ja nein
- Wird ggf. auf die Bildung von Nutzungsprofilen und das Widerspruchsrecht des Bürgers hingewiesen? ja nein
- Wird ggf. auf Verfahren hingewiesen, die eine spätere Identifikation des Bürgers ermöglichen (z. B. Cookies, Web-Bugs)? ja nein
- Erfolgt die Unterrichtung vor bzw. mit Beginn des Nutzungsvorgangs? ja nein
- Ist die Unterrichtung jederzeit und von allen Seiten aus abrufbar? ja nein
- Ist die Datenschutzerklärung P3P-kompatibel? ja nein

8.5.1.3 Informationen über Weitervermittlung (s. Kap. 5.1.3)

- Wird eine Weitervermittlung zu einem anderen Anbieter – soweit eine solche erfolgt – angezeigt? ja nein
- Ist die Information auffällig und für den durchschnittlichen Bürger verständlich? ja nein
- Werden externe Werbe-Banner gekennzeichnet? ja nein

8.5.2 Materielle Rechtmäßigkeit der Datenverarbeitung (s. Kap. 5.2)

8.5.2.1 Erhebung, Speicherung und Auswertung von Nutzungsdaten (s. Kap. 5.2.1)

- Werden Nutzungsdaten erhoben und gespeichert? ja nein
- Sind die Daten für die Erbringung oder Abrechnung des Dienstes erforderlich – d. h. kann das Angebot ohne die Erhebung von Nutzungsdaten genutzt werden? ja nein
- Ist der Zweck für die Erhebung der Nutzungsdaten bestimmt? ja nein
- Werden die Daten nur für diesen Zweck erhoben und verarbeitet? ja nein
- Werden die Nutzungsdaten unmittelbar nach Beendigung der Nutzung gelöscht? ja nein

8.5.2.2 Erhebung, Speicherung, Nutzung von Bestandsdaten (s. Kap. 5.2.2)

- Beschränkt sich die Erhebung und Speicherung der Bestandsdaten auf diejenigen Daten, die zur Erfüllung der in der Zuständigkeit der Behörde liegenden Aufgabe erforderlich sind? ja nein
- Sind die Zwecke der Erhebung und Verarbeitung der Bestandsdaten im Vorhinein bestimmt? ja nein
- Werden Daten auf freiwilliger Basis erhoben? ja nein
- Wird der Bürger über die Verwendung solcher, auf freiwilliger Basis erhobenen Daten informiert? ja nein
- Wird darauf verzichtet, die Erbringung der Dienstleistung an die Angabe nicht erforderlicher Daten bzw. an die Einwilligung in eine zweckfremde Nutzung dieser Daten zu koppeln? ja nein

8.5.2.3 Einwilligung des Bürgers (s. Kap. 5.2.3)

- Werden Bestands- oder Nutzungsdaten auf der Grundlage einer elektronischen Einwilligung erhoben, gespeichert oder genutzt? ja nein
- Erfolgt die Einwilligung durch bewusste und eindeutige Handlung des Bürgers? ja nein

- Wird bei elektronischer Einwilligung ohne gesicherte Authentisierung des Bürgers auf einem anderen Kommunikationskanal eine Bestätigung an den Bürger gesendet (confirmed opt-in) oder eine zusätzliche Bekräftigung durch den Bürger abgefordert (double opt-in)? ja nein
- Ist der Inhalt der Einwilligungserklärung klar und verständlich formuliert? ja nein
- Ist die Einwilligungserklärung besonders hervorgehoben, soweit sie zusammen mit anderen Erklärungen abgegeben wird? ja nein
- Ist die Einwilligung tatsächlich freiwillig? Wird insbesondere die Nutzung des Dienstes nicht von der Einwilligung in die Nutzung der Daten für andere Zwecke abhängig gemacht, soweit kein anderer Zugang zu diesem Dienst möglich ist? ja nein
- Wird die Einwilligung protokolliert? ja nein
- Ist der Inhalt der Einwilligung jederzeit abrufbar? ja nein
- Ist die Einwilligung jederzeit widerrufbar? ja nein
- Wird der Bürger über seine Möglichkeit des Widerrufs mit Wirkung für die Zukunft unterrichtet? ja nein

8.5.2.4 Übermittlung von Bestands- und Nutzungsdaten an Dritte (s. Kap. 5.2.4)

- Wird auf eine Übermittlung von Bestands- oder Nutzungsdaten an Dritte vollständig verzichtet? ja nein
- Werden Bestandsdaten an öffentliche Stellen nur unter Einhaltung von § 15 BDSG übermittelt? ja nein
- Werden bei der Übermittlung von Bestandsdaten an nicht-öffentliche Stellen die Vorgaben des § 16 BDSG eingehalten? ja nein

8.5.2.5 Pseudonyme Auswertung von Bestands- und Nutzungsdaten (s. Kap. 5.2.5)

- Werden Nutzungsprofile erstellt? ja nein
- Ist die Erstellung von Profilen aus zwingenden behördlichen Gründen erforderlich? ja nein
- Ist technisch und organisatorisch sichergestellt, dass die Nutzerprofile nur unter einem Pseudonym geführt werden? ja nein

- Wird der Bürger auf sein Widerspruchsrecht hingewiesen? ja nein
- Beschränken sich die Nutzungsprofile auf zulässige Zwecke (Werbung, Marktforschung oder bedarfsgerechte Gestaltung des Dienstes)? ja nein
- Wird gewährleistet, dass die unter einem Pseudonym gespeicherten Nutzerprofile nicht mit den identifizierenden Angaben des Bürgers zusammengeführt werden? ja nein
- Ist dem Bürger die Inanspruchnahme des Dienstes möglich, wenn er der Verwendung seiner Daten zu Nutzungsprofilen widersprochen hat? ja nein
- Wird die Möglichkeit angeboten, mittels Cookie-opt-out das Auslesen persönlicher Interessen bzw. Vorlieben per Cookies und damit die Erstellung von Profilen ohne zusätzliche Browser-Konfiguration zu verhindern? ja nein

8.5.2.6 Speicherung und Löschung von E-Mails (s. Kap. 5.2.6)

- Werden bei der Speicherung von E-Mails die allgemeinen Voraussetzungen zur Speicherung personenbezogener Daten beachtet? ja nein

8.5.2.7 Cookies, Web-Bugs und ähnliche nutzeridentifizierende Techniken (s. Kap. 5.2.7)

- Wird auf die Verwendung von Cookies vollständig verzichtet? ja nein
- Erfolgt eine Unterrichtung des Bürgers über das Ob und Wie der Verwendung von Cookies bzw. Web-Bugs? ja nein
- Erfolgt die Unterrichtung tatsächlich bevor Cookies gesetzt werden? ja nein
- Ist die Unterrichtung jederzeit und von allen Seiten abrufbar? ja nein
- Ist die Unterrichtung über die Verwendung inhaltlich und rechtlich korrekt und vollständig? Wird der Bürger auch darüber informiert, dass ohne sein Zutun Nutzungsprofile gebildet und beim nächsten Aufruf der Seite verwendet werden? ja nein
- Wird ggf. auf die Bildung von Nutzungsprofilen und das Widerspruchsrecht des Bürgers hingewiesen? ja nein
- Wird das Verfahren erläutert, das zur Anpassung der Angebots-Inhalte auf die persönlichen Interessen verwendet wird? ja nein

- Wird erläutert, in welchem Umfang, zu welchem Zweck und wie lange Cookies und ähnliche Erkennungsdateien gespeichert werden (Verfallsdatum) und welche Inhalte in diesen Dateien gespeichert werden? ja nein
- Wird - soweit implementiert - auf die Möglichkeit eines „Cookie-opt-out“ Verfahrens hingewiesen? ja nein

8.5.2.8 Wahrung der Betroffenenrechte (s. Kap. 5.2.8)

- Sind auf den Web-Seiten entsprechende Formulare oder andere elektronische Möglichkeiten zur Auskunftserteilung, Berichtigung oder Löschung von Bestandsdaten vorgesehen? ja nein
- Ist gewährleistet, dass der Betroffene auch ohne aktive Nachfrage benachrichtigt wird, wenn Daten über ihn ohne seine Kenntnis erhoben werden? ja nein
- Ist gewährleistet, dass die Auskunft nur an den Berechtigten erteilt wird (Sicherung der Authentizität)? ja nein
- Erfolgt eine Verschlüsselung bei elektronischer Auskunftserteilung? ja nein
- Wird bei elektronischer Auskunftserteilung die unberechtigte Kenntnisnahme der Auskunft durch unberechtigte Dritte ausgeschlossen? ja nein
- Wird die Auskunft auch hinsichtlich der Herkunft der personenbezogenen Daten erteilt? ja nein
- Umfasst die Auskunft auch die Empfänger, denen personenbezogene Daten übermittelt wurden? ja nein
- Ist gewährleistet, dass auch Auskunft über den Zweck der Speicherung der personenbezogenen Daten gegeben wird? ja nein
- Wird auch Auskunft über solche Daten des Bürgers erteilt, die unter einem Pseudonym gespeichert sind? ja nein
- Umfasst die Auskunft auch die Daten, die durch den Diensteanbieter auf dem Rechner des Bürgers abgelegt wurden (z. B. in Cookies)? ja nein
- Ist gewährleistet, dass unrichtige Bestands- oder Nutzungsdaten entsprechend den gesetzlichen Vorgaben berichtigt, gesperrt oder gelöscht werden? ja nein
- Ist gewährleistet, dass unrichtige personenbezogene Daten, die als Inhalt des Dienstes veröffentlicht werden, berichtigt, gesperrt oder gelöscht werden? ja nein
- Erfolgt die Löschung bzw. Sperrung personenbezogener Bestands- und Nutzungsdaten unverzüglich? ja nein

- Ist gewährleistet, dass personenbezogene Daten auch physikalisch gelöscht werden? ja nein

8.5.3 Datensparsamkeit (s. Kap. 5.3)

- Ist der Web-Server so konfiguriert, dass eine IP-nummernbezogene und damit personenbezogene Protokollierung der Nutzungsdaten unterbleibt? ja nein
- Werden personenbezogene Nutzungsdaten frühestmöglich anonymisiert bzw. pseudonymisiert? ja nein
- Ist die Nutzung von Diensten, die keiner Identifizierung bedürfen (z. B. Download von Formularen) anonym möglich? ja nein
- Ist die Nutzung von Diensten, die keiner direkten Identifizierung bedürfen (z. B. bei Gruppenzugehörigkeit), unter Pseudonym möglich? ja nein

8.6 Verantwortlichkeit für Inhalte (s. Kap. 6)

8.6.1 Verantwortlichkeit für eigene und fremde Inhalte (s. Kap. 6.1)

- Erfolgt eine klare und für den Bürger nachvollziehbare Trennung von eigenen und fremden Inhalten? ja nein
- Erfolgt eine regelmäßige Überprüfung der eigenen Webseite auf rechtswidrige Inhalte? ja nein
- Erfolgt eine Überprüfung der im eigenen Angebot vorhandenen Links auf rechtswidrige Inhalte dritter Anbieter? ja nein

8.6.2 Jugendschutz (s. Kap. 6.2)

- Wird die Kontrolle auf Rechtmäßigkeit auch auf den Bereich Jugendschutz ausgedehnt? ja nein
- Sind dem Verantwortlichen die wesentlichen Kriterien für jugendgefährdende Inhalte bekannt? ja nein
- Enthält das Web-Angebot einen Hinweis darauf, dass Jugendschutzbestimmungen eingehalten werden? ja nein

9 Autorendarstellung

Oliver Stutz, Ass.jur., datenschutz nord GmbH



Herr Stutz ist als Jurist bei der datenschutz nord GmbH (www.datenschutz-nord.de) verantwortlich für die Bereiche Teledienste- und Multimediarecht. Nach seiner Tätigkeit als Rechtsanwalt legte Herr Stutz als Justiziar eines international tätigen Kommunikationsdienste-Anbieters seinen beruflichen Tätigkeitsschwerpunkt bereits frühzeitig auf das Online-Recht. Seit Beginn des Jahres 2002 ist Herr Stutz bei der datenschutz nord GmbH für den Geschäftsbereich Datenschutzaudit verantwortlich. In diesem Rahmen hat er die u.a. internet privacy standards, ein auf Qualitätskriterien basierendes Datenschutz-Zertifikat für Online-Dienste entwickelt (vgl. hierzu auch DuD 2002, Seite 330).

Dipl. Inf. Isabella Schicktanz, Technologie-Zentrum Informatik



Frau Schicktanz ist als wissenschaftliche Mitarbeiterin im Bereich Informationsmanagement im Technologie-Zentrum Informatik der Universität Bremen (www.tzi.de) verantwortlich für die Entwicklung wissenschaftlich fundierter Konzepte für Qualifizierungsmaßnahmen im Rahmen von E-Government-Projekten unter Berücksichtigung des Lernoffice an der Verwaltungsschule der Freien Hansestadt Bremen. Dabei berät sie Lehreinheiten beim Durchführen von Schulungsmaßnahmen, entwickelt und evaluiert die Konzeption des Lernoffice und unterstützt Planungen, Implementationen und Umsetzungen von E-Government-Anwendungen.

Dr. Martin Wind, Technologie-Zentrum Informatik



Herr Dr. Wind ist Geschäftsführer des Bereichs Informationsmanagement im Technologie-Zentrum Informatik der Universität Bremen. Seine Arbeitsschwerpunkte liegen in der Entwicklung, Umsetzung und Evaluation von Maßnahmen und Konzepten in den Bereichen Verwaltungsreform und E-Government. Zuletzt hat Herr Dr. Wind u.a. das Teilprojekt zur Entwicklung signaturbasierter Online-Dienste für Studierende im Rahmen des Bremer MEDIA@Komm-Vorhabens geleitet.