



HS Bremerhaven • Juristischer Datenschutz • SS2006

Datenschutzrechtliche

Anforderungen

an das

e-Government

Gliederung

Gliederung.....	2
Einleitung.....	3
Der Begriff „e-Government“	4
Was ist e-Government?.....	5
Auszug aus Wikipedia	5
Anforderungen an das e-Government.....	8
Anforderungen der Bürger.....	8
Anforderungen der Wirtschaft.....	9
Allgemeine Anforderungen.....	11
Der Datenschutz.....	13
Die rechtlichen Rahmenbedingungen	13
Die Grundlagen.....	14
Gesetzliche Grundlagen.....	15
Datenschutz im IT-Bereich.....	18
Fazit und Kritik	19

Einleitung

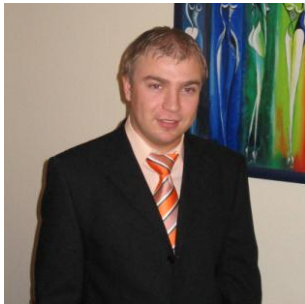
Diese Hausarbeit wurde ausgearbeitet von:



Thomas Müller

E-Mail: thomas@fivedigital.net

Matrikel-Nr.: 23876



Roman Allenstein

E-Mail: r.allenstein@gmx.net

Matrikel-Nr.: 23950

Der Begriff „e-Government“



Wer heute „e-Government“ als Suchargument bei Google eingibt, bekommt ein Informationsangebot, das aus mehr als 60 Mio. Einzelpositionen besteht, davon allein 3 Millionen Seiten in deutscher Sprache.



Laut Definition und der Begriffserklärungen der Bundesregierung in ihrer Initiative „Bund Online 2005“ umfasst das e-Government nicht mehr und nicht weniger als „alle Prozesse der öffentlichen Willensbildung, der Entscheidungsfindung und Leistungserstellung in Politik, Staat und Verwaltung unter weitestgehender Nutzung von Informations- und Kommunikations-Technologien“.

Bis Ende dieses Jahres sollen unter dem Label „e-Government“ in mehr als 100 Bundesbehörden 350 Dienstleistungen online verfügbar gemacht werden. Hierzu steht ein Investitionsvolumen von ca. 1,65 Milliarden Euro zur Verfügung.

Was ist e-Government?


Auszug aus Wikipedia

Der Begriff e-Government hat zwei unterschiedliche Bedeutungen:

 **Er ist im *weiteren Sinn* ein Oberbegriff von E-Administration, E-Democracy und E-Justice.**

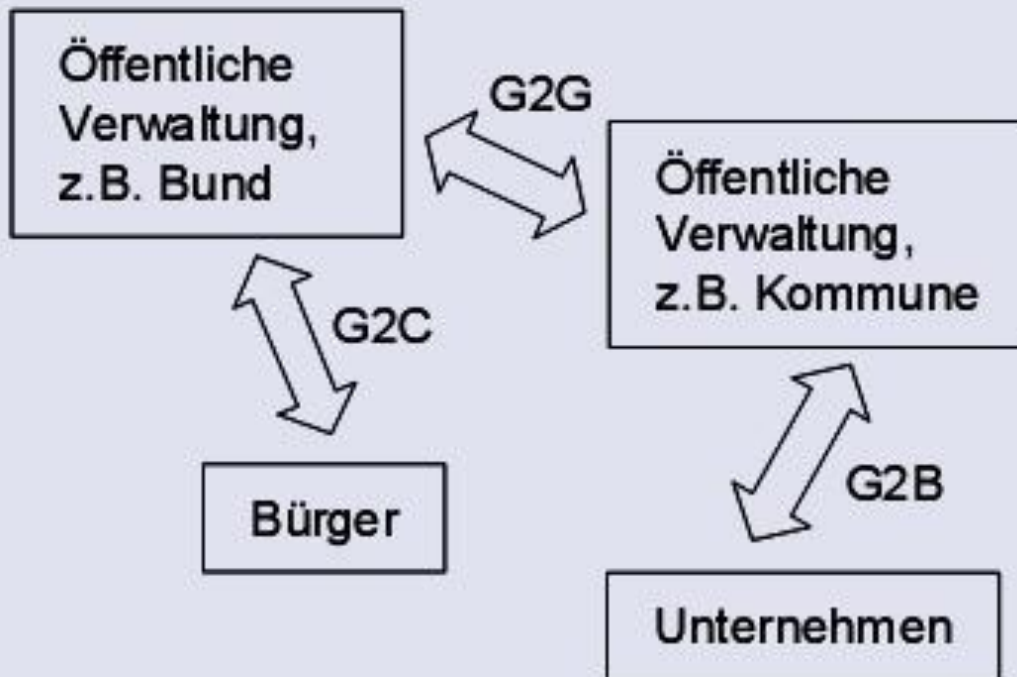
Unter e-Government im weiteren Sinn versteht man die Vereinfachung und Durchführung von Prozessen zur Information, Kommunikation und Transaktion innerhalb und zwischen staatlichen Institutionen, sowie zwischen diesen Institutionen, Bürgern und Unternehmen durch den Einsatz von Informations- und Kommunikationstechnologien.

e-Government fasst somit E-Administration (e-Government im engeren Sinn), E-Democracy und E-Justice zusammen.

 **Er ist im *engeren Sinn* ein Synonym für E-Administration, da die Begriffe E-Democracy und E-Justice bei staatlichen Institutionen außerhalb der Exekutive etabliert sind und insbesondere in der Praxis das Hauptaugenmerk des e-Governments seit langem auf die Exekutive gerichtet ist.**

Unter E-Administration oder e-Government im engeren Sinn (elektronisches Regieren und Verwalten) versteht man die Vereinfachung und Durchführung von Prozessen zur Information, Kommunikation und Transaktion innerhalb und zwischen Institutionen der Exekutive (Behörden), sowie zwischen diesen Institutionen und Bürgern (G2C), Unternehmen (G2B) und weiteren staatlichen Institutionen (G2G) durch den Einsatz von Informations- und Kommunikationstechnologien.

Dimensionen des E-Government (Dienstleistungen der Verwaltung)



Quelle: DB Research, 2005

G2C – Government to Citizen

Information

- 🏛️ Öffnungszeiten-Abfrage
- 🏛️ Touristische Information
- 🏛️ Bürgerinformationssysteme








Kommunikation

- 🏛️ Anmeldung Sperrmüll
- 🏛️ Terminabsprache mit Sachbearbeiter per E-Mail










Transaktion

- 🏛️ Kfz-Anmeldung
- 🏛️ Wohnsitz-Ummeldung
- 🏛️ Elektronische Steuererklärung

G2G – Government to Government

- Information**
-  Abfrage von Gesetzen anderer Behörden
 -  Abfragen von Kontaktinformationen
- Kommunikation**
-  Austausch personenbezogener Daten zwischen Behörden
 -  Kfz-Steuermitteilung zwischen Kommune und Finanzamt
- Transaktion**
-  Telekooperation
 -  Ressourcenmanagement
 -  Druckauftrag für Personalausweise an Bundesdruckerei

G2B – Government to Business

- Information**
-  Standortmarketing
 -  Steuerinformation
 -  Beschaffungsinformation
- Kommunikation**
-  Anfragen zu Fördergeldern
 -  Rechtliche Beratung
 -  Preisanfragen zur Beschaffung
- Transaktion**
-  Handelsregistereintrag
 -  elektronische Ausschreibungen
 -  Melderegisterauskunft

Anforderungen an das e-Government

Anforderungen der Bürger

Die Abwicklung von Behördendienstleistungen über das Internet liegt im Interesse der Bürger sogar vor der Abwicklung von Geldgeschäften, Buchung von Reisen oder der Bestellung von Eintrittskarten.

Die zahlreichen Untersuchungen zu Erwartungen und Anforderungen der Bürger an die Internetleistungen der öffentlichen Verwaltung lassen Schlussfolgerungen zu:

Der wesentliche Nutzen, den der Bürger in e-Government Dienstleistungen sieht, liegt in der **Zeiteinsparung**.

Der Bürger wünscht einen direkten und formlosen Mailkontakt mit der Verwaltung. Alle Informationen, die der Bürger im Zusammenhang mit einem Verwaltungsvorgang benötigt, werden online und in einer für den Bürger verständlichen Form erwartet. Alle Formulare und Verzeichnisse von Ansprechpartnern werden vorausgesetzt.

Insbesondere bei der Antrags- und Genehmigungsstellung sowie im Finanzbereich wird ein Online-Zugriff deutlich gefordert.

Die Abwicklung von öffentlichen Dienstleistungen soll über verschiedene Zugangskanäle wie Internet, Bürgerbüro und Call-Center erfolgen und sich dem Bürger integriert darstellen.

Die sichere Abwicklung von Online-Dienstleistungen ist für den Großteil der Bürger eine zwingende Voraussetzung für eine umfassende Nutzung von e-Government-Dienstleistungen und Basis für den Austausch vertraulicher Informationen.


Anforderungen der Wirtschaft


Mehr als 80% der Unternehmen erwarten durch eine elektronische Kommunikation mit der öffentlichen Hand eine wesentliche Steigerung der Qualität und Geschwindigkeit von Prozessen. So versprechen sich über 60% der Unternehmen durch eine schnelle Umsetzung von e-Government deutliche Kosteneinsparungen. Somit wird für die Unternehmen die Effizienz in der Zusammenarbeit mit dem öffentlichen Sektor zu einem Wettbewerbsvorteil, so dass der jeweilige Standort durch e-Government-Dienstleistungen gestärkt werden kann.


Nahezu 80% der Unternehmen sind bereit, bei Vorhandensein von benötigten Dienstleistungen auf einer sicheren und handhabbaren Plattform einen elektronischen Datenaustausch mit dem Staat innerhalb der kommenden drei Jahre zu realisieren. Unternehmensvertreter weisen deutlich darauf hin, dass eine effiziente Umsetzung von e-Government mit einer Modernisierung der Verwaltung einhergehen muss. Nicht mehr zeitgemäße Abläufe und vielfältige Medienbrüche verlangsamen Prozesse und erzeugen hohe Personalkosten bei den Unternehmen.

Die Wirtschaft sieht die elektronische Signatur als Basis nutzbringender Prozesse und erwartet deutliche Vereinfachungen im Bereich der elektronischen Signatur. Der erste Schritt wird hier von der Verwaltung erwartet. Gespräche mit Vertretern von Unternehmensverbänden haben dieses deutlich unterstrichen.

Werden Firmen nach den Dienstleistungsangeboten befragt, die sie sich von der Verwaltung wünschen, zeigen sich vor allem Schwerpunkte in den Bereichen der allgemeinen Kommunikation, Steuer und Abgaben sowie Recht:

 **Kommunikation:** Die Korrespondenz mit der Verwaltung sollte grundsätzlich über E-Mail erfolgen. Die Unternehmen wünschen gezielte Informationen über bestehende Onlineangebote als auch die Bereitstellung eines allgemeinen Informationsdienstes über Neuigkeiten und Änderungen.



 **Finanzen:** Alle unternehmensrelevanten Steuern und Abgaben sollten komplett online abgewickelt werden können. Beispiele sind der digitale Zugriff auf die eigenen Steuerkonten, digitale Abfrage der Freistellungsbescheinigung und Gewerbeanmeldung. Zudem besteht der Wunsch zur Online-Abwicklung von Spezialsteuern.

 **Recht:** Es besteht der Wunsch nach einem verstärkten Angebot an Informationen und intelligenten Recherchemöglichkeiten über Gesetze, Verordnungen und Richtlinien. Zudem sollten die rechtsverbindlichen öffentlichen Register und Verzeichnisse online abrufbar bzw. einsehbar sein. Befragungen hinsichtlich der Priorität einzelner Dienstleistungen zeigen, dass aus der Sicht der Branchen unterschiedliche Schwerpunkte gesetzt werden. Hier zeigt sich, dass eine enge Zusammenarbeit mit den Branchen bei der Gestaltung von Online-Diensten für die Wirtschaft von hoher Bedeutung ist.

Allgemeine Anforderungen

Das Datenschutzrecht fordert von e-Government-Prozessen ein Höchstmaß an rechtlicher Transparenz und gibt den Rahmen für Sicherheitskonzepte vor.

Das europäische wie auch das darauf basierende deutsche Datenschutzrecht sind u. a. durch zwei Grundprinzipien geprägt:

 Das Prinzip der eindeutigen Verantwortungszuweisung und
 das Prinzip der Transparenz.


Jede verantwortliche Datenverarbeitende Stelle darf nur diejenigen personenbezogenen Daten und auch nur in derjenigen Art und Weise verarbeiten, zu der sie durch Gesetze oder Verträge/Einwilligungen befugt worden ist.


Hieraus leiten sich die konkreten Zulässigkeitstatbestände zur Erhebung, Speicherung, Zweckbindung, Übermittlung usw. ab. Weiterhin müssen die Prozesse für den Betroffenen nachvollziehbar ablaufen, soweit eine heimliche Datenverarbeitung nicht ausdrücklich gesetzlich zugelassen ist. Das bedingt eine (dezentrale) Registrierung aller automatisierten Verfahren und Datenbestände, um das Recht der Betroffenen auf Auskunft, auf Berichtigung, auf Sperrung, Löschung usw. gewährleisten zu können.


Im Ergebnis darf es in der öffentlichen Verwaltung keinen personenbezogenen Datenbestand geben, für dessen Inhalt nicht die Verantwortung festgelegt wurde und der bei der zuständigen Behörde registriert ist. Diese scheinbar konservative Sichtweise ist ein Regulativ für den ansonsten zu befürchtenden Wildwuchs der automatisierten Informationsverarbeitung.

Wenn externe Dienstleister in die Verwaltungsabläufe oder die technische Realisierung eingeschaltet werden, sind schriftliche Verträge, klare Weisungen und Kontrollen durch die verantwortliche Stelle obligatorisch.

Dies bedeutet, dass viele der derzeit aktuellen e-Government-Projekte, die auf der Kooperation

 zwischen einzelnen Behörden,

 zwischen ganzen Verwaltungsbereichen (mehrere Ressorts einer Landesverwaltung),

 zwischen dem Land und den Kommunen oder gar

 zwischen Ländern

basieren, erst dann realisiert werden können, wenn die Trägerschaft (Zuständigkeit, Verantwortung) für die dabei entstehenden Datenbestände und die ablauforganisatorischen Infrastrukturkomponenten geklärt ist.


Als Beispiele sind in diesem Zusammenhang zu nennen:

 zentrale Verzeichnisdienste,

 PKI einschließlich der Zertifizierungsdienste,

 zentrale virtuelle Poststellen,

 Portale,

 Vordruckserver,

 E-Mail-Providing,

 Content-Providing,

 Sprachnetze,


 Datennetze,


 Bezahldienste.


Der Datenschutz


Die rechtlichen Rahmenbedingungen

Auf der Basis von Planungen, die seit 1997 laufen, haben der Bundes- und die Landesgesetzgeber ihr Verwaltungsverfahrenrecht vor einigen Jahren so fortgeschrieben, dass einem umfassenden e-Government (scheinbar) nichts mehr im Wege steht. Im Landesverwaltungsgesetz wird z. B. festgestellt,

 dass die Übermittlung elektronischer Dokumente zulässig ist, soweit seitens des Empfängers ein entsprechender Zugang eröffnet wurde (§ 52a Abs. 1 LVwG),

 dass die durch eine Rechtsvorschrift angeordnete Schriftform durch elektronische Dokumente mit einer qualifizierten Signatur ersetzt werden kann (§ 52a Abs. 2 LVwG),

 dass für elektronische Verwaltungsakte die dauerhafte Überprüfbarkeit durch eine qualifizierte Signatur vorgeschrieben werden kann (§ 108 Abs. 4 LVwG) und

 dass automatisiert erstellte Verwaltungsakte keiner Unterschrift bedürfen (§ 108 Abs. 6 LVwG).

Leider zeigt die Praxis, dass es zusätzlich zu den allgemeinen Bestimmungen des Verwaltungsverfahrenrechts noch einer Vielzahl bereichsspezifischer Rechtsanpassungen bedarf. Für den Bereich der Justiz ist gar ein spezielles Justizkommunikationsgesetz auf den Weg gebracht worden, das u. a. die rechtlichen Rahmenbedingungen für den elektronischen Datenaustausch zwischen Gerichten und Anwälten regeln soll.

Die Grundlagen

Zu beachten ist, dass es kein spezielles e-Government Gesetz, gibt, wie es z.B. seit 2004 eines in Österreich der Fall ist. Die datenschutzrechtlichen Rahmenbedingungen für den Datenschutz bei e-Governmentprojekten in der Bundesrepublik basieren also auf den vorhandenen Gesetzen.


Als erste und wichtigste Gesetze sind ohne Zweifel Der Artikel 1, Absatz 1 des Grundgesetzes zu zitieren

Artikel 1 Abs. 1 Grundgesetz "Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt."


Artikel 2 Abs. 1 Grundgesetz "Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Diese bilden den Grundstein für den Datenschutz. Jeder Mensch hat das Recht darauf, zu bestimmen welche Daten über ihn gesammelt werden dürfen und welche nicht. Einschränkungen des Grundrechtes auf informationelle Selbstbestimmung sind nur aufgrund eines Gesetzes möglich, welches

 dem überwiegenden Allgemeininteresse dient,

 die Voraussetzungen für die Einschränkung und den Umfang dieser Einschränkungen klar und verständlich für den Bürger regelt,

 dem Gebot der Normenklarheit entspricht und

 dem Grundsatz der Verhältnismäßigkeit beachtet [Vgl.: Bundesbeauftragter für Datenschutz, BfD-Info 1, Bonn 2004, S. 12].

Dies bedeutet, dass nur das absolute Minimum an Daten über das Individuum gesammelt werden darf, diese Sammlung einen bestimmten und definierten Zweck verfolgt und nicht für andere Zwecke verwendet werden darf, sowie entsprechende Kontrollmöglichkeiten zum Schutz der Rechte für den Einzelnen ergriffen werden.

Gesetzliche Grundlagen

Die Sicherheitsvorschriften des Datenschutzrechts sind zwar nicht speziell auf e-Government-Prozesse zugeschnitten. Sie sind jedoch so konkret formuliert, dass ihre Auswirkungen auf die betreffenden Projekte recht leicht abgeleitet werden können. Dies mag der nachfolgende Katalog verdeutlichen:

Für jedes Verfahren ist ein Sicherheitskonzept zu erstellen (§ 6 Abs. 1 DSVO).

Es ist darzustellen, welche technischen und organisatorischen Maßnahmen unter Berücksichtigung der tatsächlichen örtlichen Gegebenheiten getroffen wurden, um die Datensicherheit zu gewährleisten.

Für besonders „sensible“ Verfahren sind Risikoanalysen anzufertigen (§ 6 Abs. 2 DSVO).


In den Risikoanalysen ist zu beschreiben, welche Sicherheitsrisiken aus welchen Gründen nicht oder nur zum Teil durch die getroffenen Sicherheitsmaßnahmen ausgeschlossen werden können.

Alle Verfahren sind zu dokumentieren (§ 3 DSVO).

Die eingesetzten Programme und ihre Beziehungen zueinander sind darzustellen. Die Dokumentation muss für sachkundige Personen in angemessener Zeit nachvollziehbar sein.

Es besteht eine Pflicht zur Authentifizierung der Administratoren und der Benutzer der IT-Systeme (§ 6 Abs. 1 LDSG).

Nur wenn Unbefugte daran gehindert werden, das IT-System zu aktivieren, sind unzulässige Administrationstätigkeiten zu unterbinden (z. B. das Einschleusen von Würmern und Trojanern).

 **Es muss eine Abgrenzung zwischen der Administrationsebene und der Benutzerebene bestehen (§ 6 Abs. 2 Satz 1 LDSG).**

Administratoren dürfen Software ändern, Benutzer dürfen sie nur aktivieren.

 **Es muss einer unbefugten Kenntnisnahme und Verarbeitung der Daten durch Administratoren entgegengewirkt werden (§ 5 Abs. 1 Satz 2 Nr. 2 LDSG).**

 **Unter Vertraulichkeitsgesichtspunkten ist ein interner oder externer Administrator kein Neutrum.**

 **Die Arbeit der Systemadministratoren ist zu kontrollieren (§ 6 Abs. 2 Satz 2 LDSG).**

In Anbetracht der sicherheitstechnischen Tragweite der Aktivitäten von Systemadministratoren haben sie einen Anspruch darauf, dass sie durch regelmäßige Kontrollen der Korrektheit ihrer Arbeit von der Alleinverantwortung entlastet werden. Wie das zu geschehen hat, lässt der Gesetzgeber allerdings offen.

 **Es ist ein korrekter Konfigurationsplan zu erstellen und fortzuschreiben (§ 8 Abs. 1 DSVO).**


Hardware, die nicht im Konfigurationsplan bzw. Geräteverzeichnis registriert ist, darf nicht genutzt werden.

 **Die „offiziell“ einsetzbare Software ist in einem Verzeichnis zu erfassen (§ 8 Abs. 2 DSVO).**

Nicht registrierte Software ist zu deaktivieren, weil sie nach dem Willen der Behörde offensichtlich nicht genutzt werden soll.

 **Es ist zu dokumentieren, für welche Mitarbeiter welche Nutzungsrechte freigeschaltet worden sind (§ 8 Abs. 4 DSVO).**

Die Dokumentation muss für Dritte lesbar sein, die Darstellung der Systemparameter reicht nicht. Die Historie der Zugriffstabellen ist fünf Jahre aufzubewahren.

 **Es ist ein Verzeichnis zu führen, aus dem hervorgeht, wer von wann bis wann welche Administrationsrechte hatte (§ 8 Abs. 5 Satz 1 DSVO).**

Auch hierfür gilt eine fünfjährige Aufbewahrungsfrist.

 **Es ist ein Systemlogbuch zu führen (§ 8 Abs. 5 Satz 2 DSVO).**

Es muss Aussagen enthalten über

- den Zeitpunkt der ändernden Zugriffe auf die Betriebssystemebene,
- die Gründe hierfür,
- die veranlassende und die ausführende Person,
- die Art der Änderung und
- den Zeitpunkt der Kontrolle des Logbuches und die kontrollierende Person.


 **Es dürfen nur von der verantwortlichen Stelle freigegebene Verfahren in Produktion gehen (§ 5 Abs. 2 Satz 2 LDSG i.V.m. § 7 DSVO).**


Nicht der Administrator trägt die Verantwortung für die Korrektheit eines automatisierten Verfahrens, sondern das Behördenmanagement, das auch für entsprechende Tests zu sorgen hat.

Datenschutz im IT-Bereich


Datenschutz und IT-Sicherheit sind zwei Seiten der gleichen Medaille: Nur wenn die IT-Geräte, auf denen personenbezogene Daten gespeichert sind, entsprechend geschützt werden, ist auch der Datenschutz sichergestellt.


Im BDSG ist dies in § 9 und im Anhang zu § 9 geregelt. Demnach sollen entsprechende geeignete technische und organisatorische Maßnahmen getroffen werden, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, einen Schutz zu gewährleisten. Es werden acht Kategorien aufgezählt:


 **Zutrittskontrolle:** Unbefugten ist der Zutritt zu entsprechenden Datenverarbeitungsanlagen zu verwehren.


 **Zugangskontrolle:** keine Nutzung der Datenverarbeitungsanlagen durch Unbefugte (i.d.R. durch Login und Passwort).


 **Zugriffskontrolle:** Einsatz einer Berechtigungsstruktur (z.B. Benutzerrechte).

 **Weitergabekontrolle:** keine Veränderung, Einsichtnahme, Löschung von Daten bei ihrer elektronischen Übertragung, ihres Transports oder Speicherung.

 **Eingabekontrolle:** es muss nachträglich festgestellt werden können, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden.











 **Auftragskontrolle:** personenbezogene Daten, die im Auftrag verarbeitet würden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.


 **Verfügbarkeitskontrolle:** personenbezogene Daten sind gegen zufällig Zerstörung oder Verlust zu schützen (insbes. durch Sicherungskopien).

 **Zweckbindungsgebot:** personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden.

Fazit und Kritik

Uns ist klar, dass unsere Hausarbeit nur einen kleinen Einblick in die komplexe Fachwelt des e-Government und des Datenschutzes gibt. Die Welt des Datenschutzes hat viele Facetten und um ein erfolgreiches e-Government Projekt zu realisieren, muss man wirklich sehr genau und präzise arbeiten und alle juristischen Anforderungen erfüllen. Während unserer Arbeit haben stellen wir uns einige Fragen, die wir als Kritik und Fazit anfügen wollen.

-  Wie lange ist die Lesbarkeit elektronischer Dokumente zu gewährleisten?
-  Wie geht man mit dem Faktum um, dass es von einem elektronischen Dokument endlos viele Originale geben kann?
-  Kann man alle Mitarbeiter der öffentlichen Verwaltung arbeits- oder dienstrechtlich verpflichten, elektronische Unterschriften abzugeben, ohne dass sie das System (PKI) überhaupt verstehen?
-  Mit welcher Technik wird „What you see is what you sign“ realisiert?
-  Wie funktioniert das Nachsignieren nach Fristablauf?
-  Was passiert, wenn (kriminelle) Personen bewusst ihre Signaturkarten (Private Key) untereinander austauschen, um ein e-Government-System zu korrumpieren?
-  Welche Anforderungen sind an die Personalisierung von Signierkarten zu stellen?
-  Reicht eine PIN als „Ein-Aus-Schalter“ aus oder braucht man zwingend biometrische Merkmale?
-  Wann und wie müssen IT-Systeme, mit denen verbindliches e-Government abgewickelt wird, evaluiert und versiegelt werden?
-  Welcher rechtlichen Fiktionen bedarf es, um bei hochautomatisiert ablaufenden Verarbeitungsprozessen unter Einschaltung von „Dienstleister-Kaskaden“ eine Zurechenbarkeit von Verwaltungshandeln zu gewährleisten?

 Wie müssen derartige Verarbeitungsprozesse dokumentiert werden, damit sie die „verantwortliche Stelle“ (Begriff aus der EG-Datenschutzrichtlinie) verstehen und verantworten kann?

Fazit: Auch wenn e-Government aus Sicht des Datenschutzes kein spezielles Problem darstellt, ist auf rechtlichem Gebiet noch viel Detailarbeit zu leisten, bevor es mit dem e-Government richtig losgehen kann.


Quellen


Für die Ausarbeitung unserer Hausarbeit haben wir folgende Quellen genutzt.

 Wikipedia – www.wikipedia.org/de

 Google – www.google.de

 BUND - http://www.bfd.bund.de/DE/Home/homepage_node.html

 E-Government: Großes Potenzial nicht ausreichend genutzt; Deutsche Bank Research; 2002.

 E-Government B2G-Anforderungen der Wirtschaft; IEB in Kooperation mit der IHK; 2002.