Datenschutzaspekte von e-Government mit besonderem Bezug auf das eGOV-Projekt

Michael Sonntag[*)] und Maria Wimmer[+)]

[*)] Institut für Informationsverarbeitung und Mikroprozessorentechnik, Universität Linz
[+)] Institut für Angewandte Informatik, Universität Linz
sonntag@fim.uni-linz.ac.at, mw@ifs.uni-linz.ac.at

Abstract: Die Umsetzung von e-Government - im besonderen von one-stop Government - wirft eine Reihe rechtlicher Fragen auf. So wird durch ein one-stop Portal ein Teil der Verfahrensschritte an das zentrale Front-office ausgelagert. Aufgrund des föderalistischen Systems in europäischen Ländern sind gesetzlich verankerte Zuständigkeiten, Verantwortlichkeiten und Kompetenzen verwaltungstechnisch und organisatorisch anzupassen, um das one-stop Prinzip im Cyberspace zu ermöglichen. Nicht zuletzt müssen Fragen des Datenschutzes und des Zugriffs auf lokale Datenbestände in den vernetzten Behörden gut überlegt und gesetzlich geregelt werden.

Keywords: e-Government, Datenschutz, one-stop Government, Föderalismus

Einleitung

Online one-stop Government ist eine aktuelle Entwicklung öffentlicher Verwaltungen, ihre Leistungen und Informationen an einem zentralen Zutrittspunkt im Cyberspace zugänglich zu machen. Dabei werden Angebote aus verschiedenen Ebenen des Staates und der Verwaltung eingebunden.
Die Umsetzung dieses Konzeptes erfordert, dass Daten nicht mehr nur in einem einzelnen Amt bzw. Bereich verfügbar gemacht und verarbeitet werden. Eine übergreifende technische Infrastruktur ist notwendig, welche die Behörden vernetzt und den Zugriff auf Daten in unterschiedlichen Behörden über einen zentralen Zutrittspunkt ermöglicht. So können beispielsweise online Formularfelder im nationalen Portal beim Aufruf des Bürgers vorab mit Daten aus verschiedenen Quellen gefüllt werden.

Mit one-stop Government stellt sich die Frage des Datenschutzes in besonderer Weise. Denn ohne dieses "Data-Sharing" gehen Vorteile wie z.B. Erleichterungen für den Bürger oder eine konsistente Datenhaltung verloren.

In diesem Beitrag werden Datenschutzaspekte nebst verwandten Problemen näher untersucht. Insbesondere wird die Thematik[1] aus Sicht eines laufenden Projektes zur Implementierung einer integrierten Plattform für online one-stop Government[2] durchleuchtet, welches im Abschnitt 2 vorgestellt wird. Darauf aufbauend wird die Problematik zentraler Portale in einem föderalistischen Staat aus Sicht rechtlicher und verwaltungstechnischer Grundlagen diskutiert (Abschnitt 3). Weiters werden Probleme bei großen Datenmengen wie etwa das Doubletten-Problem und die Eindeutigkeit von Personenkennzeichnungen angesprochen (Abschnitt 4). Schließlich werden in Abschnitt 5 Aspekte des Datenschutzes bei der online Bezahlung angesprochen. Eine kurze Zusammenfassung in Abschnitt 6 rundet den Beitrag ab.

Das eGOV-Projekt

Das Projekt eGOV[2] (vgl. [6], [10]) ist ein von der EU gefördertes zweijähriges Forschungs- und Technologie-Entwicklungsprojekt im 5. Rahmenprogramm der EU, welches im Juni 2001 startete. Die Partner stellen einen ausgewogenen Mix aus öffentlichen Verwaltungen, Forschungsinstitutionen und privaten Serviceprovidern aus Deutschland, Finnland, Griechenland, Österreich und der Schweiz dar.

Das Hauptziel von eGOV ist die Entwicklung einer integrierten Plattform für die Realisierung von *online one-stop Government*. Diese eGOV Plattform stellt für die Kunden des öffentlichen Sektors einen allgemeinen und global zugänglichen Eintrittspunkt zu allen elektronisch angebotenen Informationen und Leistungen der öffentlichen Verwaltung dar. Die Benutzer sind sowohl private Bürger wie Unternehmen als auch die öffentlichen Institutionen selbst. Die Navigation durch das Portal ist nach Lebenslagen bzw. Geschäftssituationen strukturiert und ermöglicht den Zutritt zu den Dienstleistungen der einzelnen Behörden.

Bei der Umsetzung dieser integrierten online one-stop Government Plattform wird ein ganzheitlicher Entwicklungsansatz angewendet (vgl. [9]). Neben technischen, benutzerspezifischen, prozessrelevanten und sicherheitstechnischen Faktoren werden besonders auch organisatorische und rechtliche Aspekte durchleuchtet. Letztere stellen den Schwerpunkt nachfolgender Diskussion dar.

Zentrale one-stop Government Portale und Föderalismus

Das Konzept des one-stop Government Portals basiert auf einem zentralen Zutrittspunkt für alle Dienstleistungen des Staates und der Verwaltung, welcher zumeist vom Bund gehostet und betreut wird. Verwaltungsverfahren, die auf kommunaler bzw. regionaler Ebene erledigt werden, werden ebenfalls in dieses zentrale Portal einge-

[1] Für die Erörterungen wird die bestehende Gesetzeslage in Österreich angenommen, da viele Bereiche auch einer anderen Regelung durch Gesetze zugänglich sind, wobei jedoch teilweise Gründe nach Art. 8 Abs. 2 EMRK erforderlich wären.

[2] eGOV (An integrated Platform for realising online one-stop Government, IST-2000-28471), http://www.egov-project.org/

gliedert. Dies ist bei föderalistischen Staaten aufgrund verschiedener Zuständigkeitsbereiche ein Problem. Es stellt sich die Frage, wer wann für welche Datenverarbeitungen in welcher Rolle verantwortlich ist.

Die gemeinsame Verarbeitung von Daten und Leistungen im one-stop Portal stellt einen Informationsverbundsystem (§ 4 Z 13 DSG [1]) dar, da mehrere Auftraggeber existieren, welche die Daten gemeinsam nützen. Direkter Zugriff auf Daten anderer Einheiten besteht zwar meist nicht, doch können diese für die Personalisierung von Website-Bereichen auch anderer als der des Inhabers bzw. zum Füllen fremder Formulare verwendet werden. Gem. § 50 DSG ist ein gemeinsamer Betreiber zu bestellen, welcher der tatsächliche Verarbeiter sein sollte.

Anwendbarkeit der Datenschutz-Richtlinie bzw. des Datenschutzgesetzes

Für das one-stop Konzept stellt sich die Frage, ob die Datenschutz-Richtlinie (DS-RL [2]) bzw. das Datenschutzgesetz (DSG) [1] anwendbar sind. Die DS-RL betrifft auch den öffentlichen Bereich (ohne bestimmte Gebiete wie z. B. Landesverteidigung). Das DSG ist hier ähnlich. Zusätzlich sind Gesetzgebung und Gerichtsbarkeit ausgenommen (für eGOV und allg. wegen meist vorhandenem Rechtsweg kein Problem[3]). Dem öffentlichen Bereich ist jede Verarbeitung durch Auftraggeber öffentlichen Rechts zuzuordnen[4].

Verschiedene Rollen

Gem. § 10 DSG darf ein Dienstleister nur dann eingesetzt werden, wenn dieser ausreichende Gewähr für rechtmäßige und sichere Datenverarbeitung bietet. Dies kann bei Durchführung durch den Bund (bzw. einer von diesem beauftragten Stelle) angenommen werden. Zusätzlich ist eine Vereinbarung (s. u.), sowie das Einholen von Informationen über erfolgte Maßnahmen (ev. Beschreibung in der Vereinbarung; keine Überprüfung nötig) erforderlich. Zwei Rollen sind im Betrieb zu unterscheiden:

- Bund – Eigene Angelegenheiten: Der normale Fall; eigene Daten werden selbst oder von einem selbst gewählten Dienstleister verarbeitet.
- Bund – Länder-/Gemeinde-Angelegenheiten: Der Bund wird als Dienstleister[5] für Länder und Gemeinden tätig und nimmt für die technische Durchführung wiederum selbst einen Dienstleister in Anspruch. Eine Vereinbarung über jede einzelne Datenverarbeitung ist erforderlich.

[3] Gegenbeispiel: In Österreich ist der Rechnungshof der Gesetzgebung zuzuordnen, was in der Vergangenheit bereits zu Datenschutz-Problemen geführt hat.

[4] Selbst wenn sie in privatwirtschaftlicher Form erfolgt, z. B. Förderungsvergabe. Auch schlichte Hoheitsverwaltung ist inbegriffen [4], wie etwa der Betrieb eines Web-Portales.

[5] Der Bund wird hier nur im Rahmen des § 11 bzw. § 4 Z 4 DSG verantwortlich (sofern er dies nicht auf den Sub-Dienstleister weiterüberwälzen kann). Der Verantwortliche kann nach Art. 2 Abs d DS-RL auch per Gesetz bestimmt werden.

Datenverwendung

Bei der Verwendung von Daten aus einem anderen Ursprungsbereich ist technisch zu unterscheiden, ob eine Referenz darauf oder eine Kopie (z. B. beim Füllen von Formularen mit bekannten Daten) verwendet wird. In ersterem Falle findet bei jeder Abfrage eine Datenübermittlung statt, während bei zweiterer u. U. gar keine erfolgt. Im Falle der Verwendung von Referenzen auf Daten anderer Datenanwendungen ist die Zustimmung des Bürgers erforderlich. Werden die Daten hingegen nur ins Formular eingesetzt, so ist dies nicht nötig[6]. Vom Datenschutz gesehen ist daher eine Kopie einer Referenz vorzuziehen. Die Ausnahme des § 8 Abs 4 Z 2 DSG (wesentliche Voraussetzung zur Aufgabenerfüllung) ist hier nicht anzuwenden, da die Datenverarbeitung zwar für die eigentliche Behörde (Land/Gemeinde) wesentlich und gesetzlich vorgesehen ist, sie aber für den Bund als Portalbetreiber nicht zutrifft. Wird ein zentrales one-stop Portal gesetzlich vorgesehen[7], so ist diese Ausnahme aber anzuwenden.

Vereinbarungen über die Durchführung

Um ein Bürgerportal wie eGOV auf eine rechtliche Grundlage zu stellen, ist ein Bund - Länder Übereinkommen erforderlich. Dies kann im Rahmen eines Gliedstaatsvertrages (Art 15a B-VG) erfolgen. In Bezug auf ein solches Portal muss exakt unterschieden werden, welche Vorgangsschritte wem zuzuordnen sind (Kompetenz, Zuständigkeit der Erledigung). Das Ausfüllen von Formularen entspricht bspw. dem Parteienverkehr und kann autonom geregelt werden (Amtsstunden). Die Verwendung des Portals als Ermächtigung zum Entgegennehmen für die Behörde ist derzeit in Österreich[8] schon möglich.

Automatisierte Verfahren

Sind Urkunden oder andere Beweismittel elektronisch vorhanden und das Verfahren einfach (kein Ermessensspielraum), so kann eine automatische Erledigung in direkter Interaktion mit dem integrierten und zuständigen Back-office System erfolgen. Hier stellt sich eine verfassungsmäßige Problematik (Bescheidbegriff). So ist gemäß VfGH [8] bei automationsunterstützt erstellten Bescheiden zwar keine Person als Genehmigender zu nennen (Unterschrift ist nach AVG nicht nötig), doch muss der Bescheid tatsächlich von der zuständigen Behörde veranlasst worden sein.
Weiters muss die Behörde, welcher der Bescheid rechtlich zuzurechnen ist und die ihn daher zu verantworten hat, auch tatsächlich imstande sein, auf den automationsunterstützt ablaufenden Vorgang der Ausfertigung bestimmenden Einfluss zu nehmen. Dies ist dennoch kein Problem, da auch bisher [7] davon ausgegangen wurde, dass eine Behörde die Bescheiderstellung auslagern darf, solange sie selbst die Kon-

[6] Die Weitergabe erfolgt durch den Bürger selbst und auch die Abfrage für das Einsetzen geschieht im Auftrag des Betroffenen selbst, dem dies als Hilfestellung angeboten wird.

[7] Zu einem ähnlichen Problem (verschiedenste Aufgaben von Gemeinden, die nicht konkret gesetzlich vorgesehen sind), siehe schon [3] zur fast gleichen Regelung im früheren DSG.

[8] In www.help.gv.at, da vom Bund betrieben.

trolle behält. Wichtig ist daher besonders, dass keine andere Behörde oder Person willensbildend (d. h. mit der Möglichkeit, das Ergebnis zu beeinflussen) mitwirkt.

Doubletten: Doppelte Daten und doppelte Personen

Bei Doubletten werden entweder einer Person zwei Datensätze oder zwei Personen einem Datensatz[9] zugeordnet. Unterschiedliche Daten für eine Person entstehen, wenn keine komplette Datenintegration[10] vorliegt (z.B. Schreibvarianten, doppelte Erfassung, etc.). Mehrere Personen werden dann einem Datensatz zugeordnet, wenn sie viele identische Daten besitzen (z. B. Name und Geburtsdatum). Doubletten sind problematisch, wenn eine automatische Auswertung erfolgt, da dort nur wenige Felder verglichen werden und eine Übereinstimmung der restlichen Daten anschließend angenommen wird.

Eindeutige Personen-Nummer/-Kennzeichnung

Werden bei händischer Abwicklung Daten kontrolliert und Unterschiede (z. B. Schreibung mit ae statt ä) ignoriert, so ist dies bei automatischer Suche meist unmöglich. Abhilfe in Österreich schafft hier die ZMR-Zahl, welche seit 1.3.2002 für jeden Bürger eindeutig vorhanden ist. Nach wie vor problematisch bleibt:

- Ist die ZMR-Nummer unbekannt, muss die Person nach anderen Merkmalen gesucht werden mit der Gefahr, dass die Person falsch zugeordnet wird.
- Eine ZMR-Nummer macht nur Sinn, wenn jede Datenbank darauf umgestellt wird, was sehr hohe Kosten verursacht. Auch die Zuteilung an die Bürger ist komplex.
- Eindeutige Speicherung bedingt, dass keine lokalen Kopien mehr existieren dürfen. Es ist daher bei jedem Datenzugriff eine Übertragung vom zentralen Server nötig.
- Die ZMR-Zuordnung bringt psychologische Probleme: Person und Zahl werden leicht gleichgesetzt; Personen ohne solche laufen Gefahr „nicht zu existieren".

Auch aus Datenschutzsicht ist dieses Modell bedenklich: Ist die Personennummer bekannt, können alle Daten einfach abgefragt werden.[11]

Doubletten und Webportale

Das Problem der Erkennung mehrerer Benutzer als eine Person ist in Webportalen bekannt: Die Identifizierung erfolgt oft über Cookies, welche meist nur pro Computer einmalig sind. Auch werden Personen mehrfach registriert. Bei einem e-Government Portal wie eGOV ist dies unzulässig und muss verhindert werden, da schon bei Perso-

[9] Vgl. hierzu auch § 49 DSG

[10] Komplette Datenintegration bedeutet, dass jedes Datum nur absolut einmal gespeichert ist

[11] Hier wird in Österreich für die elektronische Abwicklung ein Verfahren angewendet, das aus der ZMR-Zahl und dem eindeutigen Schlüssel des beantragten Verfahrens eine eindeutige ID berechnet, welche nur für dieses Verfahren des Beantragenden schlüssig ist. Jedoch ist es nicht möglich aus dieser Nummer Rückschlüsse auf die ZMR des Antragstellers zu machen.

nalisierung und unbefugtem Zugang Informationen bekannt werden. Die Identifizierung könnte über eine eindeutige Nummer (s.o.) oder andere Arten[12] erfolgen. Noch besser ist jedoch, grundsätzlich auf die Erhebung unnötiger Daten zu verzichten [5].

Datenschutz und Bezahlung

Früher wurden Gebühren für Verwaltungsverfahren mit Stempelmarken als anonyme Zahlungsweise abgegolten. Bei elektronischer Bezahlung, wie sie in einem Portal mit Transaktionen erforderlich ist, werden jedoch durch den Zahlungsvorgang selbst zusätzliche Informationen wie Kreditkarten- oder Kontonummern preisgegeben. Dies ist ähnlich wie in e-Commerce, doch ist dort die Missbrauchsgefahr geringer, da weniger sonstige Informationen zur Verfügung stehen. So kann etwa bei einer Überweisung einfach überprüft werden, wer tatsächlich bezahlt hat (Kontoinhaber). Zumindest eine Verbindung zum Verfahren und dem Zahlungszweck ist aber erforderlich (Vermeidung der mehrfachen Nutzung einer Zahlung). Eine automatische Prüfung sollte möglich sein. Die Zusage österreichischer Banken, eine elektronische Zahlungsbestätigung (im Gegensatz zu den bisher ausschließlichen Auftragsübernahmebestätigungen) anzubieten kann dieses Problem nicht lösen. Hierbei handelt es sich um einen elektronischen „Erlagschein“ mit digitaler Signatur der Bank, der alle üblichen Daten erhält. Dieser ist sinnvoll für den Zahlenden selbst, der hiermit einen Beleg erhält. Für eine Weitergabe ist er aus Datenschutzsicht jedoch nicht ideal.

Hier - aber auch bei anderen Zahlungsarten - wäre daher ein zweiter Beleg wünschenswert, auf dem nur verminderte Informationen aufscheinen: Idealerweise würden nur angegeben, dass ein bestimmter Betrag zu einem gewissen Termin für ein einzelnes Verfahren (identifiziert durch eine Verfahrensnummer und ein Ziel-Konto o. ä.) bezahlt wurde, und zwar bei irgendeiner Bank. Insbesondere letzteres stellt ein Problem dar, da dies eine zentrale Stelle benötigen würde, welche als eine Art „Anonymizer“ (wie für Mail oder WWW), dient. Dieser Zusatzbeleg könnte ansonsten ohne zusätzlichen Aufwand von der durchführenden Bank ausgestellt werden.

Zusammenfassung

Um ein one-stop Government Portal - sei es nun ein virtuelles oder physisches one-stop Bürgerbüro - umzusetzen, ist es wichtig, die gesetzlichen und verwaltungstechnischen Rahmenbedingungen ebenfalls anzupassen. Vor allem wird eine Entwicklung in die eine Richtung (z.B. nur technisch ausgerichtet) ohne gleichzeitig auch die Änderungsmaßnahmen in der anderen Richtung vorzunehmen, nicht zum gewünschten Erfolg führen. Leider ist man sich dessen in vielen laufenden e-Government Projekten nicht wirklich bewusst.

Im eGOV Projekt wird versucht, auf diese Interdependenzen Rücksicht zu nehmen. So werden aufgrund der technischen Zielvorstellungen für eine integrierte online one-stop Government Plattform auch die rechtlichen Änderungserfordernisse diskutiert.

[12] z.B. mit Nutzerkennung und Passwort, elektronische Signaturkarten usw.

Die wichtigsten in Bezug auf die österreichische Rechtslage sind in diesem Beitrag angesprochen. So wurde die Problematik des föderalistischen Staates und das Erfordernis verwaltungstechnischer Anpassungen aufgerollt (v.a. in Bezug auf die Zuständigkeitsregelung für Verfahren bei der Einbringung über ein zentrales, gesamtstaatliches Portal). Darüber hinaus ist der Datenschutz ein wichtiges Thema in einem Informationsverbundsystem, wie es die eGOV integrierte Plattform für one-stop Government darstellt.

Schließlich ist anzumerken, dass der Erfolg und die Akzeptanz eines zentralen one-stop Government Portals im Cyberspace stark von einer "smarten" (aufeinander abgestimmten) Entwicklung technischer, organisatorischer, verwaltungstechnischer, personeller und rechtlicher Komponenten abhängen. Gerade im europäischen Raum spielen der Datenschutz und rechtlich festgelegte Zugriffsregelungen auf persönliche Daten eine wesentliche Rolle.

Literatur

[1] DSG (Datenschutzgesetz): Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) BGBl. I Nr. 165/1999 idF BGBl. I Nr. 136/2001

[2] DS-RL (Datenschutz-Richtlinie): Richtlinie 95/46/EG des Europ. Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl L 281/31 23.11.1995

[3] Josef Hofinger (Hg.): Probleme des Datenschutzes in den Gemeinden. Wien: Verlag Jugend & Volk, 1982

[4] Christoph Mallmann: Datenschutz in Verwaltungs-Informationssystemen. München: Oldenburg 1976

[5] Michael Sonntag: Engineering for Privacy. Reducing personal information and complying to privacy laws. In: Hofer Christian, Chroust Gerhard (Ed.): IDIMT-2002. 10th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2002 (erscheint)

[6] Efthimios Tambouris: An Integrated Platform for Realising Online One-Stop Government: The eGOV Project, in: Proceedings der DEXA Internationalen Workshops, IEEE Computer Society Press, Los Alamitos, CA, 2001, 359-363

[7] VfSlG 8844/1980, B 122/79 vom 18.6.1980

[8] VfSlG 11590/1987, G 110/87 vom 26.12.1987

[9] Maria A. Wimmer: Integrated service modeling for online one-stop Government. EM – Electronic Markets, special issue on e-Government, Vol. 12, No. 3, 2002 (erscheint).

[10] Maria Wimmer, Johanna Krenner: Next Generation One-Stop Government Portale: das Projekt "eGOV". In Bauknecht, Brauer, Mück (eds.): Informatik 2001, Tagungsband der GI/OCG Jahrestagung, Band 1, OCG, Wien, 2001, 277 - 284.