

**Der Landesbeauftragte  
für den Datenschutz und  
für das Recht auf Akteneinsicht**



**Internationales Symposium  
Informationsfreiheit und Datenschutz**

**Transparenz und E-Government in  
Mittel- und Osteuropa**

**10./11. November 2003**

Dokumentation

**Akteneinsicht und  
Informationszugang  
Potsdamer Materialien  
Band 3**



**Internationales Symposium  
Informationsfreiheit und Datenschutz  
Transparenz und E-Government in  
Mittel- und Osteuropa**

10./11. November 2003 in Potsdam

Veranstaltung des  
Landesbeauftragten für den Datenschutz  
und für das Recht auf Akteneinsicht  
in Zusammenarbeit mit der  
Alcatel SEL Stiftung für Kommunikationsforschung  
und der Deutschen Gesellschaft für  
Recht und Informatik e.V.  
mit Unterstützung der DaimlerChrysler AG

Dokumentation

In der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ sind bisher erschienen:

Band 1: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz; 25./26. Oktober 1999

Band 2: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union; 8./9. Oktober 2001

Band 3: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz - Transparenz und E-Government in Mittel- und Osteuropa; 10./11. November 2003

## **Impressum**

Herausgeber: Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg  
Stahnsdorfer Damm 77, Haus 2  
14532 Kleinmachnow

Dezember 2003

Telefon: +49 33203 356-0  
Fax: +49 33203 356-49

E-Mail: [Poststelle@LDA.Brandenburg.de](mailto:Poststelle@LDA.Brandenburg.de)  
Internet: <http://www.lida.brandenburg.de>

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Gallus Druckerei KG, Berlin

## Inhalt

	Seite
Vorwort	5
Dr. Alexander Dix	
Eröffnung / Opening	7
Dr. Herbert Knoblich	
Grußwort zur Eröffnung / Greeting	11
Jann Jakobs	
Grußwort zur Eröffnung / Greeting	15
Dr. Bruno Baeriswyl	
Eine einheitliche Gesetzgebung für Datenschutz und Informationszugang im Rahmen eines E-Government- Rechtssetzungskonzepts / A Uniform Data Protection and Access to Information Legislation within the Legislative E-Government Framework	17
Burckhard Nedden	
Datenschutzgerechtes E-Government / Privacy-Compliant E-Government	33
A. Erhardt Ewert	
Erfahrungen aus dem Projekt e-LoGo / The e-LoGo Project Experience	67
Marit Hansen	
Identitätsmanagement und E-Health / Identity Management and E-Health	95



Andriy Pazyuk	
Transparenz und E-Government in der Ukraine / Transparency and E-Government in the Ukraine	135
Prof. Dr. Murat Aşkar	
E-Government-Projekte und ihre Auswirkungen in der Türkei / E-Government Projects and their Impacts in Tur- key	143
Ivar Tallo	
Informationszugang als Voraussetzung für E-Government: Das Beispiel Estland / Access to Information as the Foun- dation of e-Government: The Case of Estonia	173
Jernej Rovšek	
Projekte zur Informationsfreiheit und zum E-Government in Slowenien / Freedom of Information and the E-Government Projects in the Republic of Slovenia	187
Krzysztof Głomb	
Grenzübergreifendes E-Government: Handeln anstatt zu reden – der Ansatz des Verbands „Städte im Internet“ / E-Government across the Borders: How to Act, not just Talk about – „Cities on Internet“ Association Approach	197
Franz Blaser	
Geoinformationssysteme und Informationszugang / Geo- graphic Information Systems and Access to Information	213
Prof. Dr. Roland Traunmüller	
Die internationale Dimension des E-Government: Die EU- Fallstudie Como / The International Dimension of E-Government: The EU Como Case Studie	243

## **Vorwort**

Seit 1999 lädt der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht alle zwei Jahre zum Internationalen Symposium „Informationsfreiheit und Datenschutz“ nach Potsdam ein. Dieser dritte Band der „Potsdamer Materialien zu Akteneinsicht und Informationsfreiheit“ dokumentiert die Vorträge und Präsentationen des Symposiums, das am 10. und 11. November 2003 in der brandenburgischen Landeshauptstadt stattfand und sich mit „Transparenz und E-Government in Mittel- und Osteuropa“ befasste. Dabei berichteten Fachleute aus EU-Mitgliedstaaten wie Deutschland und Österreich, aber auch aus zentraleuropäischen Ländern, die am 1. Mai 2004 der Union beitreten werden wie Estland, Slovenien und Polen, und schließlich Experten aus der Schweiz, der Ukraine und der Türkei über den jeweiligen Entwicklungsstand in ihren Ländern.

Dabei wurde trotz der teilweise erheblichen nationalen Unterschiede deutlich, dass elektronische Verwaltungsdienstleistungen zunehmend nicht mehr nur als Mittel zur Effektivierung und Verschlinkung des Staatsapparates verstanden, sondern zugleich als Chance zur Stärkung der bürgerschaftlichen Teilhabe begriffen werden. E-Government ist ohne eine Zusammenschau von Informationsfreiheit und Datenschutz nicht sinnvoll zu verwirklichen. Nur wenn die Bürgerinnen und Bürger sicher sein können, dass ihnen der Zugang zur virtuellen Verwaltung möglichst barrierefrei eröffnet wird, ohne dass sie an der Vertrauenswürdigkeit dieses zusätzlichen Kommunikationsweges zweifeln müssen, werden sich elektronische Behördendienste auch durchsetzen.

An dieser Stelle danke ich dem Landtag Brandenburg und den beiden Mitveranstaltern, der Alcatel SEL Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik e. V., insbesondere aber meinen Mitarbeiterinnen und Mitarbeitern sehr herzlich für ihre Unterstützung bei der Vorbereitung und Durchführung dieses Symposiums.

Dr. Alexander Dix  
Landesbeauftragter für den Datenschutz  
und für das Recht auf Akteneinsicht



**Dr. Alexander Dix,**  
Landesbeauftragter für den Datenschutz  
und für das Recht auf Akteneinsicht

## **Eröffnung des Internationalen Symposiums**

Ich heiÙe Sie alle sehr herzlich bei diesem Internationalen Symposium zu Informationsfreiheit und Datenschutz willkommen. Ich tue dies zugleich im Namen der beiden Mitveranstalter, der Alcatel SEL Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik.

Der Ministerpräsident des Landes, den wir um ein Grußwort gebeten hatten, ist leider ebenso verhindert wie sein Stellvertreter. Ich nehme nicht an, dass dies ein Zeichen dafür ist, dass die Landesregierung dem Thema dieser Konferenz nur geringe Bedeutung beimisst. Immerhin hat sie in diesem Jahr die Aufstellung eines „Masterplans E-Government“ beschlossen, von dem sicher heute und morgen noch die Rede sein wird.

Ich freue mich, dass zum dritten Mal seit 1999 zahlreiche ausgewiesene Experten aus dem In- und Ausland unserer Einladung gefolgt sind, um das Verhältnis zwischen Informationsfreiheit und Datenschutz zu diskutieren. Sie kommen zum einen aus Ländern, die der Europäischen Union schon länger angehören, nämlich Deutschland und Österreich; zum anderen aus drei Ländern, die im Mai nächsten Jahres der Union beitreten werden, und zwar aus Polen, Estland und Slowenien, und schließlich aus drei Ländern, die diesen Schritt bisher nicht getan haben, aber möglicherweise eines Tages tun werden, nämlich der Schweiz, der Ukraine und der Türkei.

Unter den Teilnehmern begrüÙe ich zudem weitere Datenschutzbeauftragte aus Mittel- und Osteuropa, insbesondere den Präsidenten der tschechischen Datenschutzbehörde, sowie die Kolleginnen und Kollegen aus den anderen Bundesländern.

Informationsfreiheit und Transparenz in der elektronischen Verwaltung ist ein Thema, bei dem es sich besonders lohnt, über den Tellerrand zu schauen. Der frühere polnische Botschafter in Deutsch-

land, Janusz Reiter, hat bei dem Festakt zum 10-jährigen Jubiläum der Verfassung des Landes Brandenburg im vergangenen Jahr gesagt: „Je offener eine Gesellschaft ist, desto besser sind ihre Chancen im Wettbewerb“. Das gilt für Gesellschaften ebenso wie für ihre Verwaltungen. Auch Verwaltungsbehörden stehen im Wettbewerb miteinander etwa um die schnellsten und transparentesten Genehmigungsverfahren bei Ansiedlungsvorhaben der Wirtschaft.

Gegenwärtig verhandeln die Regierungen aller, auch der im kommenden Jahr der Union erst beitretenden Mitgliedsländer über eine Europäische Verfassung. Dabei gibt es zahlreiche ungeklärte Fragen, über die noch Einigkeit erzielt werden muss. Über eines besteht aber bereits jetzt Übereinstimmung zwischen den jetzigen und zukünftigen Mitgliedstaaten der Union: über den Katalog der Grundrechte und Grundfreiheiten aller Bürgerinnen und Bürger der Union. Zu ihm zählen auch die beiden thematischen Säulen unseres Symposiums - Informationsfreiheit und Datenschutz. Eine zivile europäische Informationsgesellschaft ist ohne diese beiden Grundpfeiler nicht vorstellbar.

Vor diesem Hintergrund werden die Referentinnen und Referenten heute und morgen die Chancen und Risiken der elektronischen Verwaltung erörtern. „E-Government“ wird landläufig als Königsweg zur Effizienzsteigerung in der staatlichen und kommunalen Verwaltung und vielleicht auch als eine Art Konjunkturprogramm für die EDV-Branche angesehen. Diese Sichtweise erscheint mir allerdings zu eng. Uns liegt daran, dass darüber hinaus die Aspekte der demokratischen Teilhabe und des sparsamen Umgangs mit personenbezogenen Daten bei der Vernetzung der Verwaltung untereinander und mit den Bürgerinnen und Bürgern verstärkt in den Blick genommen werden. Verwaltungsmodernisierung ist kein Selbstzweck, sondern sie soll den Bürgerinnen und Bürgern erkennbare Vorteile bringen. Deshalb sollten alle, die gegenwärtig in Brandenburg und anderswo neue E-Government-Anwendungen entwerfen, sich mit der Frage auseinandersetzen, welche Auswirkungen ihre Konzepte auf die Transparenz und den Datenschutz haben werden. Das Ergebnis einer solchen grundrechtsorientierten Technikfolgenabschätzung ist nicht notwendig negativ. Vielmehr ist es denkbar, dass netzbasierte Dienstleistungen der Verwaltung größere Kommunikationssicherheit und Transparenz ermöglichen als bisher. Wo immer sich solche Chancen eröffnen, sollten sie genutzt werden.

Nur auf diese Weise und durch nutzerfreundlich gestaltete Angebote können die Bürgerinnen und Bürger für solche Vorhaben gewonnen werden.

Dies gilt für alle Projekte, die jetzt im Rahmen der E-Government-Strategie des Landes Brandenburg verfolgt werden, angefangen vom Brandenburger Online Amt über das webbasierte Fortbildungsmanagement für das Verwaltungspersonal im Projekt „Smart-learning“ bis hin zum Kabinetts-Informationssystem der Staatskanzlei.

Dabei lohnt es sich, auch die Erfahrungen kennen zu lernen, die unsere ausländischen Nachbarn in diesem Bereich gesammelt haben. Lassen Sie mich nur das Beispiel Estlands herausgreifen, das morgen noch näher beleuchtet werden wird: Viele Entscheidungen der estnischen Regierung werden unmittelbar, nachdem sie getroffen worden sind, noch im Sitzungssaal des Kabinetts zum Abruf ins Internet gestellt. Das estnische Beispiel ist aber noch aus einem anderen Grund interessant: Dort müssen es Unternehmen, die sich um öffentliche Aufträge bewerben, hinnehmen, dass sämtliche Angebotsunterlagen, jedenfalls nach der Vergabeentscheidung, öffentlich zugänglich sind. Auch wenn das deutsche Rechtssystem dies bisher noch nicht zulässt, ist es doch bemerkenswert, dass einige Länder, die erst an der Schwelle zur Europäischen Union stehen, über ein höheres Transparenzniveau als die Bundesrepublik verfügen. Das ist nicht nur von akademischer, sondern auch ganz praktischer Bedeutung, wenn man bedenkt, dass deutsche Unternehmen sich schon jetzt um staatliche Aufträge in Estland bewerben können.

Die Beschäftigung mit den ausländischen Erfahrungen bei der Verwaltungsmodernisierung ist auch aus einem weiteren Grund vorrangig: Die Bundesrepublik ist eines der letzten Länder in Europa, die auf der Ebene des Bundesstaates noch nicht über ein allgemeines Informationsfreiheitsgesetz verfügen. Die Informationsbeauftragten der Länder Brandenburg, Berlin, Schleswig-Holstein und Nordrhein-Westfalen haben aus diesem Grund das Jahr 2003 zum „Jahr der Informationsfreiheit“ erklärt. Unser Symposium ist die dritte von vier Veranstaltungen in diesem Jahr, die dem gemeinsamen Ziel dienen, die Bundesregierung und den Bundesgesetzgeber davon zu überzeugen, dass die Verabschiedung eines Bundesinformationsfreiheitsgesetzes überfällig ist. Ich erinnere daran, dass der

frühere Staatssekretär im Bundesinnenministerium bereits beim ersten dieser Symposien 1999 Grundzüge eines entsprechenden Gesetzentwurfs vorgestellt hat, der aber bisher die Widerstände aus Wirtschaft und Verwaltung nicht hat überwinden können.

Es besteht für mich kein Zweifel daran, dass Verwaltungsmodernisierung und E-Government nur dann Erfolg haben werden, wenn sie die informationelle Teilhabe und informationelle Selbstbestimmung der Bürgerinnen und Bürger fördern und unterstützen. E-Government ist informationszugangsfreundlich und datenschutzgerecht zu verwirklichen, und zwar im doppelten Sinn: es ist möglich und notwendig.

Das gilt gerade auch in Zeiten knapper öffentlicher Kassen. Ich sage dies im Hinblick auf den Gesetzentwurf der Landesregierung, über den gegenwärtig der Landtag berät und mit dem zur Entlastung der Kommunen die Ausübung des Rechts auf Akteneinsicht in Brandenburg eingeschränkt werden soll. Der Landtag wird – so hoffe ich – meine Empfehlungen zu diesem Entwurf berücksichtigen und das bundesweit erste Informationszugangsgesetz nicht beschneiden, zumal die Kommunen dadurch nicht wirklich entlastet würden. In Zeiten sinkender Wahlbeteiligung wäre es das falsche Signal, die Wahrnehmung von Mitgestaltungsrechten der Bürgerinnen und Bürger zu erschweren.

Wenn dieses Symposium zeigen kann, dass E-Government und Verwaltungsmodernisierung nicht allein für die effektivere Erledigung von Verwaltungsaufgaben stehen, sondern darüber hinaus die Chance bieten, den Freiheitsraum der einzelnen Menschen durch Transparenz und Datenschutz zu erweitern, dann hat es seinen Zweck erreicht.

Ich wünsche Ihnen und mir, dass uns das an diesen beiden Tagen gelingt.

**Dr. Herbert Knoblich**

Präsident des Landtages Brandenburg

## **Grußwort zur Eröffnung**

Zum diesjährigen Internationalen Symposium „Informationsfreiheit und Datenschutz“ heiße ich Sie in der schönsten Landeshauptstadt Deutschlands herzlich willkommen und überbringe Ihnen die Grüße des Landtages Brandenburg.

Sie wollen sich heute und morgen mit „Transparenz und E-Government in Mittel- und Osteuropa“ beschäftigen - damit haben Ihnen unser Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht, Herr Dr. Dix, und seine Mitveranstalter ein Thema vorgegeben, das jeder von uns zu verstehen versucht. Die eine Facette betrifft das Verhältnis der Bürgerinnen und Bürger zu den staatlichen Institutionen, die andere die bevorstehende sogenannte Ost-Erweiterung der Europäischen Union.

Als Landtagspräsident verfolge ich mit besonderem Interesse die Bemühungen um eine verstärkte Nutzung elektronischer Medien etwa bei der Vorbereitung und Durchführung von Wahlen. Ich bin sicher, dass das in Brandenburg bereits erfolgreich erprobte E-Voting eine wichtige Ergänzung eines größeren E-Government-Konzepts werden wird. Bereits bei den Bürgermeisterwahlen 2001/2002, bei der Bundestagswahl im vorigen Jahr und gerade erst bei den Kommunalwahlen sind vereinzelt amtlich zugelassene Stimmzählgeräte zum Einsatz gekommen. Wir sind augenblicklich dabei, unser Landeswahlgesetz entsprechend zu ändern, damit dies auch für Landtagswahlen möglich wird. Vielleicht können wir dadurch schneller und sicherer auswerten und zudem eine so erschreckend hohe Zahl von ungültigen Stimmen wie bei der Kommunalwahl vermeiden helfen - um eine höhere Wahlbeteiligung zu erreichen, werden wir uns zusätzliche Gedanken machen müssen.

Ich bin darüber hinaus froh, dass wir parallel zur amtlichen Landtagswahl im nächsten Jahr eine ausschließlich methodisch angelegte sogenannte Juniorwahl durchführen werden, an der sich annähernd 50 Schulen beteiligen sollen. Diese Online-Wahl am Computer, die einhergehen wird mit einer intensiven didaktischen Vorbereitung und Begleitung der Schülerinnen und Schüler, soll in erster Linie dem Üben und Erleben



von Demokratie dienen - denn in Sachen Technik machen uns die jungen Menschen allemal etwas vor.

Bis zu einer sicheren und datenschutzgerechten Stimmabgabe über das Internet bei allgemeinen Wahlen dürfte es allerdings – nicht nur aus Kostengründen – ein weiter Weg sein. Ich nenne nur eine von zahlreichen Fragen, die noch zu beantworten sind: In der athenischen Polis als der ältesten bekannten Demokratie waren die wahlberechtigten Bürger verpflichtet, nachdem sie ihre Stimme durch Einwurf einer Scherbe in die Urne abgegeben hatten, auf dem Marktplatz (Agora) als dem umgrenzten Ort der Wahl solange auszuharren, bis alle abgestimmt hatten. Nur auf diese Weise konnte seinerzeit eine doppelte Stimmabgabe ausgeschlossen werden.

Wir behelfen uns heute mit Wählerverzeichnissen, in denen die Stimmabgabe vermerkt wird, ohne die Wähler in ihrer Bewegungsfreiheit einzuschränken. Sollen Wahlen und Abstimmungen aber in offenen Netzen wie dem Internet ermöglicht werden, ist eine Grundvoraussetzung, dass die ordnungsgemäße Berücksichtigung jeder Stimme nachprüfbar ist, ohne dass das Wahlgeheimnis beeinträchtigt wird.

Diese und zahlreiche andere Probleme sind wahrscheinlich lösbar. Die Beantwortung aller Fragen muss deshalb besonders ernst genommen werden, weil hier etwas Entscheidendes auf dem Spiel steht: das Vertrauen der Wahlberechtigten in den demokratischen Prozess. Vertrauen setzt in erster Linie Transparenz voraus, die beim Einsatz von Datenverarbeitungstechnik mindestens in gleicher Weise gewährleistet sein muss wie bei der Stimmabgabe mittels Wahlzetteln und manueller Auszählung. Dies gilt in gleicher Weise auch für alle anderen Anwendungsmöglichkeiten der elektronischen Verwaltung. Die Bürgerinnen und Bürger werden sie nur annehmen, wenn ihnen die angebotenen Verfahren durchschaubar und deshalb vertrauenswürdig ist.

Der zweite Aspekt Ihres Symposiums, die Konzentration auf Mittel- und Osteuropa, führt mich zum Stichwort Ost-Erweiterung der Europäischen Union. Nachdem vor Kurzem auch die Bevölkerung Lettlands mit deutlicher Mehrheit für den Beitritt zur EU gestimmt hat, steht jetzt fest, dass am 1. Mai des kommenden Jahres zehn Staaten, darunter auch unser direktes Nachbarland Polen, Neumitglieder in der Europäischen Union werden.

Fälschlicherweise wird in diesem Zusammenhang immer wieder von einer *Erweiterung* Europas gesprochen. Aber in Wahrheit - und hier verwende ich gerne den Satz von Willy Brandt im Zuge der deutschen Vereinigung - wächst hier nur zusammen, was zusammen gehört. Und die mehr als fünfzigjährige, politisch bedingte Teilung, die durch dieses Zusammenwachsen endlich überwunden wird, sollte nun nicht erneut durch so vordergründige Einteilungen in *altes* und *neues* Europa vorgenommen werden.

Gerade beim Thema dieser Veranstaltung wird deutlich, wie groß der gemeinsame Fundus an Grundüberzeugungen zwischen den jetzt wieder zusammenwachsenden Teilen Europas ist. Das wird bei allen Schwierigkeiten in Detailfragen leider allzu oft übersehen.

Ich hoffe, dass dieses Symposium einen Beitrag zur Stärkung dieser Gemeinsamkeiten leisten kann und wünsche Ihnen in diesem Sinne interessante Diskussionen. Vielleicht finden Sie darüber hinaus noch die Zeit, sich von der Schönheit Potsdams und der Freundlichkeit seiner Bewohner zu überzeugen.



**Jann Jakobs**

Bürgermeister der Landeshauptstadt Potsdam

## **Grußwort zur Eröffnung**

Als Oberbürgermeister der Landeshauptstadt Potsdam möchte ich Sie herzlich zu Ihrem 2-tägigen Symposium, das jetzt zum dritten Mal bei uns stattfindet, willkommen heißen. Das Internationale Symposium zu Problemen der Informationsfreiheit und des Datenschutzes hat sich zu einer guten Tradition entwickelt. Dadurch wird die Wichtigkeit des Schutzes der Grundrechte auf Informationsfreiheit und Datenschutz der Bürgerinnen und Bürger Europas auch für uns Potsdamer unterstrichen.

Als Gastgeber wollen wir hierfür einen aktiven Beitrag leisten. Der Geist der Aufklärung und Toleranz des späten 17. und 18. Jahrhunderts, welcher auch Lessing und Voltaire in unsere Region führte und diese Stadt prägte, bildet einen Anknüpfungspunkt an die heutige Informationsfreiheit. Hier wird uns die Möglichkeit eröffnet, sich ohne Voraussetzungen einen Zugang zu öffentlichen Informationen zu verschaffen. Dagegen wird die Privatsphäre des Einzelnen durch den Schutz personenbezogener Daten garantiert. Letzteres harmonisierte weitestgehend erfolgreich eine Datenschutzrichtlinie der Europäischen Union. In der Frage, wie transparent aber ein Staat zu sein hat, unterscheiden sich noch die Auffassungen in Europa. Deshalb gilt es, die Diskrepanz zwischen der beispielsweise seit Jahrhunderten in Schweden realisierten Informationsfreiheit und dem diesbezüglichen Stand in der Bundesrepublik Deutschland, wo bis heute kein Informationsfreiheitsgesetz verabschiedet wurde, zu überwinden.

Die Umsetzung dieser wichtigen Ziele bedarf einer modernen Verwaltung, welche sich zeitgemäßer und effizienter Mittel bedient. Wie es der Untertitel des Symposiums andeutet, wird also Transparenz auch mit eGovernment verwirklicht. Das eGovernment bezeichnet hierbei viele Verfahren, die elektronisch eine Kommunikation zwischen einer Behörde sowie Bürgerinnen und Bürgern ermöglichen. Oftmals haben solche neuen Datenverarbeitungs-Systeme erst das Stadium eines Pilotprojektes erreicht, weil sie auf die noch selbst in

der Entwicklung befindlichen Möglichkeiten des Internets setzen. Das Internet offeriert einer unbegrenzten Zahl von Menschen einen Informationszugang.

Der erste Schritt stellt also eine fachgerechte Aufbereitung der Verwaltungsinformationen nach außen über Web-Portale dar, was die Transparenz staatlichen Handelns verbessert. So können bereits jetzt vergleichsweise kostengünstig Informationen ohne einen Personenbezug elektronisch öffentlich zugänglich gemacht werden. Die nächste Stufe repräsentiert die Abwicklung von Verwaltungsverfahren mittels elektronischer Behördenangebote. Hierbei zeigt sich jedoch, dass die Nutzerinnen und Nutzer solche Anwendungen nur akzeptieren, wenn sie ihre Daten mit einer Verwaltung ohne das Risiko eines unberechtigten Zugriffs darauf austauschen können. Ziel muss es deshalb sein, den Schutz der personenbezogenen Daten mittels sicherer Verfahren zu ermöglichen, um die Rechte der Bürgerinnen und Bürger zu wahren.

Ich möchte Ihnen noch einige Worte zum heutigen Tagungsort mitteilen:

Potsdam als ausgeprägter Kultur- und Wissenschaftsstandort entwickelt sich zunehmend in seiner nationalen und internationalen Bedeutung. So gehören große Teile der Stadt mit ihren unvergleichlichen Schlössern und Gärten zum Weltkulturerbe der UNESCO. Deshalb empfehle ich Ihnen während der Pausen des Symposiums einen Spaziergang durch die Stadt mit ihren kulturellen Schätzen, Herren- und Bürgerhäusern sowie Kirchen zu unternehmen, sich von der Schönheit bezaubern zu lassen und Inspirationen für einen längeren Besuch bei uns zu sammeln. Ja, ich hoffe, dass in vielen von Ihnen der Wunsch geweckt wird, wiederzukommen, um mehr von unserer Stadt Potsdam und der sie umgebenden reizvollen märkischen Landschaft mit ihren Wäldern, Seen, Hügeln und Sehenswürdigkeiten kennen zu lernen. Ihnen als Experten für Datenschutz, Informationsfreiheit und eGovernment wünsche ich zu diesem Symposium konstruktive Beiträge und Diskussionen sowie im Ergebnis der Tagung eine Verbesserung der Transparenz und mittels der modernen Informations- und Kommunikationstechnologien optimierte und bürgerfreundliche Verwaltungen auf höchstem Niveau in Europa.

**Dr. Bruno Baeriswyl**

Datenschutzbeauftragter des Kantons Zürich, Schweiz

## **Eine einheitliche Gesetzgebung für Datenschutz und Informationszugang im Rahmen eines E-Government - Rechtsetzungskonzepts**

### Inhaltsübersicht

1. Einleitung
2. Rechtsetzungskonzept zu E- Government
  - 2.1 Grundlage
  - 2.2 Regelungssystem
  - 2.3 Regelungsbereiche
  - 2.4 Verfahrensrecht
  - 2.5 Organisation
  - 2.6 Information
  - 2.7 Weitere Entwicklung
3. Gesetz über die Information und den Datenschutz (IDG)
  - 3.1 Ausgangslage
  - 3.2 Grundsätze und Aufbau
  - 3.3 Grundsätze im Umgang mit Informationen
  - 3.4 Bekanntgabe von Informationen
  - 3.5 Interessenabwägungen
  - 3.6 Beauftragte/r für Informationszugang und Datenschutz
4. Fazit

## 1. Einleitung

Der Kanton Zürich als der bevölkerungsreichste Kanton der Schweiz (1,3 Mio. Einwohner), der auch wirtschaftlich das ökonomische Zentrum der Schweiz bildet, hat sich von Anfang an für die Belange des E-Government gezeigt. Im Rahmen der wirkungsorientierten Verwaltungsführung (New Public Management) wurde im Einsatz moderner Informations- und Kommunikationstechnologien ein hohes Potential für eine effizientere Gestaltung des Verhältnisses zwischen Bürgerinnen und Bürgern sowie dem Staat gesehen. Diese Bemühungen wurden in verschiedenen Projekten konkretisiert und umgesetzt<sup>1</sup>.

Bei diesen Vorhaben wurde rechtzeitig gesehen, dass auch auf der Ebene des Rechts Anpassungen notwendig sein werden. Es wurde deshalb beschlossen, diese Rechtsanpassungen soweit wie möglich einheitlich anzugehen. Zu diesem Zweck wurde ein Rechtsetzungskonzept<sup>2</sup> ins Auge gefasst, das die Leitlinien für die Rechtsanpassungen aufzeigen sollte. Gleichzeitig wurde erkannt, dass das Datenschutzgesetz wegen des gesteigerten Einsatzes moderner Informations- und Kommunikationstechnologien und den damit verbundenen Risiken für die betroffenen Personen einen Reformbedarf aufwies. Außerdem verlangte das Parlament von der Regierung die Einführung des Prinzips der Öffentlichkeit der Verwaltung. Da beide Materien eng verknüpft sind, wurde entschieden, die beiden Vorhaben aufeinander abzustimmen. Damit war der Grundstein gelegt für eine einheitliche Gesetzgebung für Datenschutz und Informationszugang.

Im Folgenden werden die Leitlinien des Rechtsetzungskonzepts kurz vorgestellt, um anschließend auf die Gesetzgebung für Datenschutz und Informationszugang, das Gesetz über die Information und den Datenschutz (IDG), einzugehen.

---

<sup>1</sup> Die Projekte reichen vom Aufbau eines einheitlichen Portals ([www.zh.ch](http://www.zh.ch)) bis zur elektronischen Abstimmung (E-Voting).

<sup>2</sup> Zur Zeit liegt ein Zwischenbericht zu diesem Konzept vor (Dezember 2003).

## **2. Rechtsetzungskonzept zu E- Government**

### 2.1 Grundlage

Das Rechtsetzungskonzept ist vom Grundsatz geleitet, dass die elektronisch angebotene Information und der elektronische Verkehr mit den staatlichen Behörden möglichst niederschwellig zugänglich und möglichst umfassend zulässig sein soll. Rechtliche Bestimmungen, die dem entgegenstehen, sollen deshalb angepasst werden, oder allenfalls sind entsprechende rechtlichen Voraussetzungen zu schaffen.

Diese grundsätzliche Ausrichtung bedeutet auch, dass eine rechtliche Regulierung auf das Notwendigste beschränkt werden soll. Allerdings sollen mit der Umsetzung von E-Government nicht gleichzeitig tragende Grundsätze der Rechtsordnung in Frage gestellt werden: Auch bei E-Government sind die gleiche Sicherheit und Qualität zu gewährleisten, die bisher das Vertrauen im herkömmlichen Rechtsverkehr rechtfertigen.

Mit seiner breiten Zielsetzung greift E-Government in das gesamte staatliche Handeln ein. E-Government bedarf deshalb auch einer umfassenden Einbindung in das Rechtssystem.

### 2.2 Regelungssystem

Auf Grund der Komplexität und der unterschiedlichen Entwicklung der E-Government Projekte wurde die Frage aufgeworfen, ob ein einheitliches und systematisch abgeschlossenes Regelungssystem zu erarbeiten sei. E-Government greift nicht nur in alle Arten staatlichen Handelns ein, sondern hat auch Auswirkungen auf nahezu jeden Bereich staatlicher Tätigkeit. Der Versuch, einen derart komplexen Gegenstand mit kompakten und einheitlichen Regelungen systematisch zu fassen, läuft indessen Gefahr, ein abstraktes und vom Regelungsgegenstand isoliertes Ergebnis zu liefern. Im Kanton Zürich wurde daher vorgeschlagen, den Regelungsgegenstand beim E-Government auf der Grundlage der unterschiedlichen Arten staatlichen Handelns in drei Bereiche zu unterteilen. Für jeden Bereich sollen in je gesonderten Konzepten die rechtlichen Rahmenbedingungen erarbeitet werden.



Dabei gilt es zu beachten, dass die Regelungskompetenz vielfach nicht beim Kanton, sondern beim Bund liegt. Deshalb ist sicherzustellen, dass die kantonale Rechtsetzung mit allfälligen Spezial- oder Bundesregelungen abgestimmt wird. Des Weiteren sind die Vorgaben der Bundesverfassung zu beachten. Im Vordergrund stehen besonders die Gewährleistung des Grundsatzes von Treu und Glauben im Rechtsverkehr, die Beachtung der Anforderungen des Service Public und der Rechtsgleichheit sowie die Pflicht zu wettbewerbsneutralem Verhalten des Staats. Diese verfassungsrechtlichen Vorgaben liefern keine konkreten Regelungen, sondern erst jene Kriterien, die es bei der Festlegung von Bestimmungen für E-Government zu beachten gilt.

### 2.3 Regelungsbereiche

In Bezug auf die Rechtsetzung werden die folgenden drei Hauptbereiche unterschieden:

Erstens das Verfahrensrecht, wo der Einzelne in einer unmittelbaren rechtlichen Beziehung zum hoheitlich tätigen Staat steht. Der Abschluss oder die Beendigung des Rechtsverhältnisses, meistens aber bereits einzelne Verfahrensschritte, führen in der Regel zu einer Änderung der individuellen Rechtsposition des Betroffenen.

Zweitens die Informationstätigkeit, bei der der Einzelne häufig nicht in ein bestimmtes Rechtsverhältnis zum Staat tritt. Das bloße Abrufen von Informationen, Stellen von Anfragen, Deponieren von Feedbacks etc. stellt in der Regel lediglich einen tatsächlichen Kontakt dar, der keine Veränderung einer (individuellen) Rechtsposition bewirkt.

Den dritten Hauptbereich bildet die Organisation (Aufbau und Finanzierung), die die Aufgaben umfasst, welche zur infrastrukturellen Administration gehören.

### 2.4 Verfahrensrecht

Das elektronische Handeln des Staats im Bereich des Verfahrensrechts ist erst wenig entwickelt. Das hängt zu einem großen Teil daran, dass die Auslösung staatlicher Aktivität in der Regel unmittelbare Auswirkungen auf individuelle Rechtspositionen hat. Aus der

Optik der Sicherheit für den Rechtsverkehr mit Behörden und Gerichten ist die Frage von zentraler Bedeutung, ob und wie weit die Zulassung neuer technischer Mittel rechtlich zu regeln ist. Es stellen sich insbesondere Fragen in Bezug auf die Formerfordernisse und die Zustellungs- und Beweisregelungen. Dabei gilt es die Anforderungen an die Sicherheit wie Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit umzusetzen. Für den Entscheid, welche Formvorschriften im Verfahrensrecht gelten sollen, ist daher abzuklären, ob mit der Zulassung einer elektronischen Form die Funktion der bisherigen Formerfordernisse erfüllt werden kann. Gleichzeitig ist zu fragen, ob die jeweilige Funktion respektive Formvorschrift überhaupt aufrechterhalten werden soll und ob eventuell weitere rechtliche Bestimmungen erforderlich sind. Des Weiteren ist festzulegen, wie entscheidend die Authentizität einer Person bei einer Eingabe an die Behörden ist. Was für die erstmalige Eingabe von Bedeutung sein kann, muss nicht unbedingt auch bei weiteren der Fall sein. Für das Verfahrensrecht stehen damit grob unterteilt zwei verschiedene Formen zur Verfügung: die einfache elektronische Form (Mail, Passwörter, etc.) und die PKI - basierte digitale Signatur.

## 2.5 Organisation

Im Rahmen von E-Government stellen sich Fragen der Organisation insbesondere auf der Ebene der Sicherheit und des Datenschutzes. Sie sind deshalb auch stark mit den Verfahrensfragen verbunden. Die mit dem elektronischen Geschäftsverkehr verbundenen neuen Risiken stehen im Vordergrund. Die Rechtsetzung hat dabei – soweit nicht schon vorhanden – die notwendigen Vorgaben an die organisatorischen und technischen Maßnahmen zu formulieren. Zu beachten gelten hier auch das Wettbewerbsrecht und das Gleichheitsprinzip, insofern der Staat mit dem Setzen von bestimmten technischen Standards in Marktprozesse eingreifen kann.

## 2.6 Information

Die elektronische Information über staatliche Tätigkeiten ist weit fortgeschritten und erfasst nahezu alle Gebiete staatlicher Aktivität. Entsprechend breit ist das Spektrum des Angebots von Regierung und Verwaltung. Bei der Integration der neuen Technologien in das Informationsangebot des Staats sind diverse Fragen zu entschei-

den. So ist das Ausmaß und die Reichweite des Zugangs zu Informationen der Verwaltung zu bestimmen, sind die allfälligen Kosten für die Nutzung solcher Informationen festzulegen und ist über den Schutz personenbezogener Informationen zu entscheiden.

Diese Fragen sollen im Rahmen des Gesetzes über Information und den Datenschutz (IDG) geklärt werden, soweit nicht zumindest teilweise bereichsspezifische Regelungen notwendig sein werden.

## 2.7 Weitere Entwicklung

Der Zwischenbericht zum Rechtsetzungskonzept im E-Government zeigt die Hauptbereiche und die geplante Vorgehensweise auf, um den notwendigen rechtlichen Rahmen für die verschiedenen Vorhaben im Bereich des E-Government zu schaffen. Da das Rechtsetzungskonzept für ein bereichsweises Vorgehen plädiert, sind die weiteren Schritte insbesondere vom Fortschreiten der einzelnen E-Government-Projekte abhängig. Diese befinden sich zur Zeit eher in einer Phase der Konsolidierung, weshalb in nächster Zeit nicht mit einer großen Rechtsetzungsaktivität zu rechnen ist. Eine Ausnahme bildet dabei das Gesetz über die Information und den Datenschutz (IDG).

## 3. Gesetz über die Information und den Datenschutz (IDG)<sup>3</sup>

### 3.1 Ausgangslage

Der Kanton Zürich kennt bisher kein ausdrückliches Recht auf Zugang zu Informationen. Damit steht er hinter einer Reihe von Schweizer Kantonen, die das Prinzip der Öffentlichkeit der Verwaltung bereits eingeführt haben<sup>4</sup>. Auf Bundesebene steht das Bundesgesetz über die Öffentlichkeit vor der parlamentarischen Debatte<sup>5</sup>. In Bezug auf den Datenschutz verfügt der Kanton Zürich seit dem 1. Januar 1995 über ein eigenes Datenschutzgesetz. Obwohl dieses Gesetz erst im Jahre 1995 in Kraft getreten ist, basiert es –

---

<sup>3</sup> Die Ausführungen beziehen sich auf den Stand des Gesetzesentwurfs vom Dezember 2003.

<sup>4</sup> Gesetzliche Regelungen finden sich in den Kantonen Bern (1995), Genf (2001), Jura (2002), Solothurn (2003) und Waadt (noch nicht in Kraft). Auf Verfassungsebene eingeführt wurde es in den Kantonen Neuenburg, St. Gallen und Schaffhausen.

<sup>5</sup> Botschaft vom 12. Februar 2003 (BBl 1003, 1963).

wie auch die übrigen schweizerischen Datenschutzgesetze – noch auf der Datenschutzkonzeption der 1960er und 1970er Jahre.

Auf Grund einer parlamentarischen Initiative (Motion) wurde die Regierung beauftragt, einen Gesetzesentwurf für die Einführung des Prinzips der Öffentlichkeit vorzulegen. In einer ersten Analyse der Sachlage verabschiedete die Regierung ein Grobkonzept für eine Gesetzgebung, welches die Integration des Informationszugangs und des Datenschutzes in einem Gesetz vorsieht. Damit wurde die Chance wahrgenommen, die eng zusammenhängende Materie auf einander abgestimmt zu regeln und der konzeptionellen Reformbedürftigkeit des Datenschutzgesetzes nachzukommen. Eine Arbeitsgruppe, mit Unterstützung externer Experten, erarbeitete den nun vorliegenden Gesetzesentwurf<sup>6</sup>.

Das gewählte Vorgehen unterstreicht damit sowohl die Wichtigkeit der Information als auch des Datenschutzes in der Entwicklung unserer Gesellschaft zur Informationsgesellschaft. Im Grobkonzept wurde deshalb betont, dass es sinnvoll erscheint, die beiden Materien, die sich mehrfach überschneiden, in einem Erlass zu regeln, gehe es doch bei beiden im Kern um die Frage des Zugangs oder Nichtzugangs zu Informationen. Modellfälle einer einheitlichen Regelung sind die Gesetze der kanadischen Provinz Québec (1982) und von Ungarn (1992). In der Schweiz finden wir eine solche Verknüpfung bisher im Informations- und Datenschutzgesetz des Kantons Solothurn<sup>7</sup>. Der Grund, dass bisher nur wenige Länder über eine einheitliche Regelung verfügen, dürfte in der unterschiedlichen historischen Entwicklung der Datenschutz- und Informationszugangsgesetze liegen. Datenschutzgesetze waren eine Reaktion auf die Entwicklungen der Informations- und Kommunikationstechnologie seit Ende der 1960er Jahre, während mit den Informationszugangsgesetzen auf die ungleiche Informationsverteilung im Verhältnis zum Staat reagiert wird, verbunden mit allgemeinen Überlegungen zu einer Reform des Verhältnisses zwischen Verwaltung und Verwalteten.

---

<sup>6</sup> Siehe: [www.datenschutz.ch](http://www.datenschutz.ch)

<sup>7</sup> Das Informations- und Datenschutzgesetz (InfoDG) des Kantons Solothurn regelt allerdings lediglich die beiden Materien unabhängig von einander in einem einzigen Gesetz.

Im Entwurf für eine neue Zürcher Kantonsverfassung<sup>8</sup> ist ebenfalls vorgesehen, dass der Systemwechsel vom Geheimhaltungsprinzip zum Öffentlichkeitsprinzip vollzogen wird. Das Recht auf Zugang zu Informationen und das Recht auf Schutz der Privatsphäre sollen als Grundrechte in der Kantonsverfassung verankert werden, wobei bei letzterem lediglich eine Verweisung auf die Bundesverfassung erfolgt. Auch die Verpflichtung der Behörden, die Öffentlichkeit über ihre Tätigkeit zu informieren, soll Eingang in die Verfassung finden.

### 3.2 Grundsätze und Aufbau

Das IDG hat zum Ziel, einen einheitlichen Umgang mit Informationen sicherzustellen. Informationen sind alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. Personenbezogene Informationen (Personendaten und besondere Personendaten) werden dabei als „Teilmengen“ des Begriffs „Informationen“ behandelt<sup>9</sup>. Ein weiteres Ziel des IDG liegt im Erfassen des Lebenszyklus der Information. Im Sinne einer prozessorientierten Betrachtungsweise sollen Rahmenbedingungen für den Umgang mit Informationen von ihrer Entstehung bis zu ihrer Archivierung oder Vernichtung geschaffen werden.

§ 1 des Entwurfs des Gesetzes über die Information und den Datenschutz (IDG) lautet deshalb wie folgt:

„Dieses Gesetz regelt die Grundsätze des Umgangs der öffentlichen Organe mit Informationen.

Es hat zum Ziel

- a) beim Umgang mit Informationen die Grundrechte, insbesondere den Schutz der Persönlichkeit, zu wahren
- b) den Zugang zu Informationen zu gewährleisten
- c) die Informationstätigkeit der öffentlichen Organe zu fördern
- d) die Interessen an der Zugänglichkeit der Informationen und die privaten und öffentlichen Interessen an der Geheimhaltung auszugleichen.“

---

<sup>8</sup> Vernehmlassungsentwurf vom 26. Juni 2003. Siehe: [www.verfassungsrat.zh.ch](http://www.verfassungsrat.zh.ch)

<sup>9</sup> § 3 Abs. 2 IDG

Im Prozess der Informationsbearbeitung legt das IDG damit vier klare Zielsetzungen. Mit dem Verweis auf die Grundrechte soll insbesondere der Datenschutz gesetzlich geregelt werden. Die Gewährleistung des Zugangs zu Informationen beinhaltet ein individuelles Informationszugangsrecht. Die öffentlichen Organe sollen angehalten werden, von sich aus zu informieren. Der Interessenausgleich zwischen Zugang und Nichtzugang zu Informationen ist ein wesentlicher Bestandteil des Gesetzes.

Damit legt das Gesetz die Grundlage für die einheitliche und umfassende Regelung der Materie Informationszugang und Datenschutz. Nach allgemeinen Bestimmungen betreffend Geltungsbereich und Begriffsdefinitionen werden sodann die Grundsätze im Umgang mit Informationen, mit zusätzlichen Bestimmungen für den Umgang mit Personendaten, die Bekanntgabe von Informationen, das individuelle Informationszugangsrecht, die Interessenabwägungen (Einschränkungen), das Verfahren auf Zugang zu Informationen sowie die Aufgaben des / der Beauftragten für Informationszugang und Datenschutz<sup>10</sup> geregelt.

Diesem Aufbau folgend werden nun einzelne Bestimmungen näher beleuchtet.

### 3.3. Grundsätze im Umgang mit Informationen

Auf Grund der erwähnten Sichtweise des Gesetzes auf den Informationsprozess bezieht sich der einleitende Paragraf in diesem Abschnitt auf die Organisation der Information. Eine sachgerechte Informationsverwaltung ist Voraussetzung, dass Informationsbegehren angemessen beantwortet werden können<sup>11</sup>. Daher ist auch vor-

---

<sup>10</sup> Aufbau des Gesetzes:

- I. Allgemeine Bestimmungen
- II. Grundsätze im Umgang mit Informationen
  - a) Im Allgemeinen
  - b) Besondere Grundsätze im Umgang mit Personendaten
- III. Bekanntgabe von Informationen
- IV. Informationszugangsrecht und weitere Rechtsansprüche
- V. Einschränkungen
- VI. Verfahren auf Zugang zu Informationen
- VII. Beauftragte oder Beauftragter für Informationszugang und Datenschutz
- VIII. Strafbestimmungen
- IX. Schluss- und Übergangsbestimmungen

<sup>11</sup> § 4 IDG

gesehen, dass mittels einer Verordnung die geeigneten Maßnahmen und Findmittel für die öffentlichen Organe vorgeschrieben werden. Damit soll die Zugänglichkeit und die rasche Auffindbarkeit der Information über ihren gesamten Lebenszyklus sichergestellt werden<sup>12</sup>. Außerdem wird so auch die Nachvollziehbarkeit des Verwaltungshandelns und die Rechenschaftsfähigkeit gewährleistet<sup>13</sup>. Nach Ablauf der Aufbewahrungsfristen sind die Informationen und die Findmittel zu vernichten oder dem Staatsarchiv abzuliefern<sup>14</sup>. Auf Grund der Pflicht zur Information über Tätigkeiten von allgemeinem Interesse und nicht zuletzt auch im Hinblick auf die Wahrnehmung des individuellen Rechts auf Informationszugang, ist vorgesehen, dass Informationen über den Aufbau, die Zuständigkeiten und die Ansprechpersonen sowie ein Verzeichnis über die Informationsbestände der öffentlichen Organe publiziert und nach Möglichkeit elektronisch zugänglich gemacht werden<sup>15</sup>. Das Verzeichnis der Informationsbestände ersetzt das Register der Datensammlungen im herkömmlichen Sinne, indem in diesem Verzeichnis Informationsbestände, die Personendaten enthalten, zu kennzeichnen sind. Das öffentliche Organ hat demnach den Umgang mit Informationen so zu gestalten, dass es ihm jederzeit möglich ist, rasch, umfassend, sachgerecht und verständlich zu informieren<sup>16</sup>.

In punkto Sicherheit verlangt das IDG, dass die Informationen durch angemessene organisatorische und technische Maßnahmen zu schützen sind. Die Maßnahmen haben sich nach den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit zu richten, wobei die der Art der Information, die Art und der Zweck ihrer Verwendung sowie der jeweilige Stand der Technik zu berücksichtigen sind<sup>17</sup>.

Der Umgang mit personenbezogenen Informationen erfolgt nach den gleichen Grundsätzen, wobei der Schutz der Privatheit durch weitergehende Prinzipien gewährleistet werden soll. An erster Stelle steht der Grundsatz der Gesetzmäßigkeit. Unterschieden wird dabei der Umgang mit Personendaten und derjenige mit besonderen Per-

---

<sup>12</sup> § 5 Abs. 3 IDG

<sup>13</sup> § 5 Abs. 1 IDG

<sup>14</sup> § 5 Abs. 2 IDG

<sup>15</sup> § 13 Abs. 2 und 3 IDG

<sup>16</sup> § 4 Abs. 1 IDG

<sup>17</sup> § 7 IDG

sonendaten<sup>18</sup>. Das Bearbeiten von Personendaten ist erlaubt, sofern es zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe geeignet und erforderlich ist<sup>19</sup>. Dagegen ist für die Bearbeitung besonderer Personendaten eine hinreichend bestimmte Regelung in einem formellen Gesetz notwendig<sup>20</sup>. Soweit Personendaten erhoben werden, muss die Beschaffung für die betroffenen Personen erkennbar sein<sup>21</sup>.

Weiter wird für das Bearbeiten von Personendaten eine Zweckbindung vorgesehen, die nur durchbrochen werden kann, soweit eine gesetzliche Regelung ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall eingewilligt hat<sup>22</sup>. Zu nicht personenbezogenen Zwecken ist eine Verwendung der Daten möglich, wenn sie anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf die betroffenen Personen möglich sind<sup>23</sup>.

Unter der Marginalie „Vermeidung des Personenbezugs“ wird das öffentliche Organ verpflichtet, keine oder so wenig Personendaten wie möglich zu bearbeiten<sup>24</sup>. Soweit möglich und verhältnismäßig sind Personendaten zu anonymisieren, pseudonymisieren oder zu verschlüsseln. Damit werden auch materielle Grundlagen geschaffen, um Informationsbearbeitungen im Rahmen von Qualitätsmanagementsystem auditieren und zertifizieren zu können. Das Gesetz sieht deshalb vor, dass öffentliche Organe zur Sicherstellung der Qualität der Verfahren der Informationsverarbeitung, der Organisation und der technischen Einrichtungen unabhängige und anerkannte Stellen mit Prüfungen und Bewertungen beauftragen können<sup>25</sup>. Damit wird ein Auditierungs- und Zertifizierungsverfahren eingeführt, das sich sehr stark an die Qualitätsmanagementsystem nach ISO 9001 anlehnt und vergleichbar ist mit dem Datenschutzaudit, wie es das Bundesland Schleswig - Holstein kennt.

---

<sup>18</sup> Der Begriff „Besondere Personendaten“ löst den Begriff der „besonders schützenswerten Personendaten“ ab (siehe § 3 Abs.4 IDG)

<sup>19</sup> § 8 Abs. 1 IDG

<sup>20</sup> § 8 Abs. 2 IDG

<sup>21</sup> § 11 IDG

<sup>22</sup> § 9 Abs. 1 IDG

<sup>23</sup> § 9 Abs. Abs. 2 IDG

<sup>24</sup> § 10 IDG

<sup>25</sup> § 12 IDG



### 3.4 Bekanntgabe von Informationen

Der Informationszugang wird in drei Stufen geregelt.

Erstens: Das öffentliche Organ hat von sich aus zu informieren über alle Tätigkeiten von allgemeinem Interesse<sup>26</sup>;

Zweitens: Das öffentliche Organ gibt Personendaten bekannt, wenn bestimmte Voraussetzungen vorliegen<sup>27</sup>;

Drittens: Das öffentliche Organ gibt Informationen bekannt auf Ersuchen einer Person (Informationszugangsrecht)<sup>28</sup>.

Die Information von Amtes wegen wird unterstützt durch verschiedene Vorgaben in Bezug auf die Führung und das Zugänglichmachen von Informationsbeständen<sup>29</sup>. Die Bestimmung lässt aber ein gewisses Ermessen zu, das schon heute von den Verwaltungsbehörden auf Grund bestehender Informationspflichten unterschiedlich wahrgenommen wird. Die Bekanntgabe von personenbezogenen Informationen verlangt grundsätzlich eine entsprechende Rechtsgrundlage, die für besondere Personendaten hinreichend bestimmt in einer formellen gesetzlichen Grundlage festgehalten sein muss<sup>30</sup>. Beim individuellen Informationszugangsrecht ist auch der Zugang zu den eigenen Personendaten mit enthalten, wie es gemäss geltendem Datenschutzrecht im Auskunftsrecht statuiert ist<sup>31</sup>.

### 3.5 Interessenabwägungen

Grundsätzlich wird eine Information nicht weiter gegeben, wenn eine gesetzliche Bestimmung dies ausschließt oder wenn ein überwiegendes öffentliches oder privates Interesse besteht<sup>32</sup>. Die Aufzählungen, was öffentliche oder private Interessen sind, erfolgt im Gesetz abschließend.

---

<sup>26</sup> § 13 IDG

<sup>27</sup> § 15 IDG; § 15 IDG

<sup>28</sup> § 18 IDG

<sup>29</sup> siehe oben

<sup>30</sup> § 16 IDG

<sup>31</sup> § 17 DSG

<sup>32</sup> § 21 IDG

Ein öffentliches Interesse liegt vor,

- wenn die Information Positionen in anstehenden Vertragsverhandlungen betrifft;
- wenn die vorzeitige Bekanntgabe der Information den internen Meinungsbildungsprozess des öffentlichen Organs erheblich beeinträchtigt;
- wenn die Bekanntgabe der Information die Wirkung von Untersuchungs-, Überwachungs- oder Aufsichtsmaßnahmen gefährdet;
- wenn die Bekanntgabe der Information die Beziehungen zu einem anderen Kanton, zum Bund oder zum Ausland erheblich beeinträchtigt<sup>33</sup>.

Ein privates Interesse liegt vor,

- wenn durch die Bekanntgabe der Information die Privatsphäre Dritter beeinträchtigt wird;
- wenn durch die Bekanntgabe der Information ein Geschäfts- oder Fabrikationsgeheimnis offenbart wird<sup>34</sup>.

Soweit das öffentliche Organ auf Gesuch hin Zugang zu Informationen gewährt, hat es in der Regel innert 30 Tagen Auskunft zu erteilen. Gesuch können abgelehnt werden, wenn Informationen bereits anderweitig öffentlich zugänglich sind oder wenn ein unverhältnismässiger Verwaltungsaufwand entstehen würde<sup>35</sup>. Mit letzterem sind insbesondere Gesuche gemeint, die mit den ordentlichen personellen Mitteln und der bestehenden Infrastruktur ohne die Vernachlässigung anderer Aufgaben nicht innert nützlicher Frist zu erledigen wären.

Die Gesuche, die Personendaten, ein Geschäfts- oder Fabrikationsgeheimnis betreffen, sind den betroffenen Dritten zur Stellung-

---

<sup>33</sup> § 22 IDG

<sup>34</sup> § 23 IDG

<sup>35</sup> § 25 IDG

nahme vorzulegen<sup>36</sup>. Besondere Personendaten können nur mit der Einwilligung der betroffenen Person bekannt gegeben werden. Soweit gegen den Willen Dritter Informationen bekannt gegeben werden sollen, steht diesen der Rechtsweg offen<sup>37</sup>. Ebenso haben die gesuchstellenden Personen, deren Begehren nicht vollständig entsprochen wird, die Möglichkeit, ein Rechtsmittel zu ergreifen<sup>38</sup>.

Grundsätzlich ist für Informationsbegehren eine Gebührenpflicht vorgesehen, außer das Auskunftsbegehren betreffe die eigenen Personendaten oder es erfordere nur einen geringen Arbeitsaufwand respektive es betrifft Anfragen von Medien oder aus der Wissenschaft<sup>39</sup>. Diese Gebührenpflicht darf selbstverständlich nicht zur grundsätzlichen Einschränkung des Rechts auf Informationszugang führen. Eine zu erlassende Gebührenordnung soll dem Rechnungstragen.

### 3.6 Beauftragte/r für Informationszugang und Datenschutz

Es ist vorgesehen, den bisherigen Datenschutzbeauftragten durch einen Beauftragten für Informationszugang und Datenschutz zu ersetzen. Entsprechend ist sein Aufgabenkatalog anzupassen. Auf Grund der Einführung neuer Instrumente ist der Katalog aber auch erweitert worden.

#### Die oder der Beauftragte

- unterstützt und berät die öffentlichen Organe in Fragen des Informationszugangs und des Datenschutzes;
- berät Private und betroffene Personen über ihre Rechte;
- kontrolliert die Anwendung der Vorschriften über den Informationszugang und den Datenschutz;
- vermittelt zwischen Privaten, betroffenen Personen und öffentlichen Organen;

---

<sup>36</sup> § 27 IDG

<sup>37</sup> § 28 Abs. 2 IDG

<sup>38</sup> § 28 Abs. 1 IDG

<sup>39</sup> § 29 IDG

- informiert über Anliegen des Informationszugangs und des Datenschutzes;
- beurteilt Erlasse und Vorhaben, die den Informationszugang und den Datenschutz betreffen;
- bietet Aus- und Weiterbildungen in Fragen des Informationszugangs und des Datenschutzes an;
- beobachtet und bewertet die technologische Entwicklungen, die das Bearbeiten von Informationen betreffen;
- unterstützt die öffentlichen Organe im Bereich der organisatorischen und technischen Maßnahmen zum Schutz von Informationen und Personendaten;
- fördert die Einführung von Qualitätsstandards in der Informationsbearbeitung<sup>40</sup>.

#### **4. Fazit**

Der vorliegende Entwurf eines Gesetzes über die Information und den Datenschutz (IDG) ist nicht nur für den Kanton Zürich, sondern auch für die Schweiz wegweisend für eine einheitliche Gesetzgebung für Datenschutz und Informationszugang. Erste externe Beurteilungen zeigen, dass die kompakte und auf einander abgestimmte Regelung der beiden Materien überzeugend wirkt. Das Gesetz kommt mit lediglich 41 Paragrafen aus, inklusive der Schluss- und Übergangsbestimmungen (4 Paragrafen). Aus Sicht der öffentlichen Organe dürfte sich ein einheitlicher Erlass über die Information und den Datenschutz als eine Erleichterung im Umgang mit Informationen und Daten zeigen. Dennoch gibt es natürlich grundsätzlich kritische Stimmen gegen die Einführung des Öffentlichkeitsprinzips.

Der Gesetzesentwurf befindet sich nun in einem Konsultationsverfahren (Vernehmlassung). Nach dessen Abschluss ist geplant, das Gesetz im ersten Halbjahr 2004 zu Händen der parlamentarischen Debatte zu verabschieden. Dabei ist anzunehmen, dass es noch einige Änderungen erfahren wird. Zu hoffen aber bleibt, dass der

---

<sup>40</sup> § 32 IDG

von der Regierung gewählte Ansatz einer einheitlichen Regelung der beiden Materien in einem Gesetz aufrecht erhalten bleibt.



**Der Landesbeauftragte für den  
Datenschutz Niedersachsen**



# **„Datenschutzgerechtes eGovernment“**

**Burckhard Nedden**

Landesbeauftragter für den Datenschutz Niedersachsen

**Vortrag auf dem Internationalen Symposium  
Informationsfreiheit und Datenschutz  
des Landesbeauftragten für den Datenschutz und  
für das Recht auf Akteneinsicht Brandenburg am  
10. November 2003 in Potsdam**

# Datenschutzgerechtes eGovernment

---

## Agenda

Potentiale  
Gefahren  
Erwartungen  
Handreichung  
Handlungs-  
empfehlungen  
Ausblick

- **Potentiale von eGovernment**
- **Gefahren für Datenschutz und Datensicherheit**
- **Erwartungen und Einschätzungen der Nutzerinnen und Nutzer**
- **Handreichung „Datenschutzgerechtes eGovernment“**
- **Einige exemplarische Handlungsempfehlungen**
- **Ausblick**

# Datenschutzgerechtes eGovernment

<b>Potentiale</b>
<b>Gefahren</b>
<b>Erwartungen</b>
<b>Handreichung</b>
<b>Handlungs- empfehlungen</b>
<b>Ausblick</b>



## Definiton

eGovernment bezeichnet die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung sowie der Leistungserstellung und -abwicklung in Politik, Regierung und Verwaltung unter Nutzung der modernen Informations- und Kommunikationstechniken, insbesondere des Internet. Einbezogen ist der gesamte öffentliche Sektor.

Aus den Handlungsempfehlungen „Datenschutzgerechtes eGovernment“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder





# Datenschutzgerechtes eGovernment

---

## Potentiale

Gefahren

Erwartungen

Handreichung

Handlungs-  
empfehlungen

Ausblick

## Interaktionsformen im eGovernment

**eInformation** (Bürgerinformationssysteme,  
Web-Angebote)

**eKommunikation** (z.B. eMail-Kontakt zur  
Verwaltung)

**eTransaktion** (alle Formen des  
rechtsverbindlichen elektronischen  
Verwaltungshandelns)

# Datenschutzgerechtes eGovernment

---

## Potentiale

## Gefahren

## Erwartungen

## Handreichung

## Handlungs- empfehlungen

## Ausblick

### Die häufigsten Kontakte mit Verwaltungen:

- ca. **700 Mio** Kassenrezepte mit mehr als **900 Mio** Verordnungen
- ca. **113 Mio** Meldungen und ca. **120 Mio** Beitragsnachweise und Überweisungen der Arbeitgeber an Sozialversicherungsstellen
- über **34 Mio** Einkommensteuererklärungen
- über **15 Mio** Kfz-Neuzulassungen und Umschreibungen
- ca. **14 Mio** Anträge auf Personalausweise und Pässe
- ca. **6,5 Mio** Wohnungsan- und -abmeldungen .....



# Datenschutzgerechtes eGovernment

---

## Potentiale

## Gefahren

## Erwartungen

## Handreichung

## Handlungs- empfehlungen

## Ausblick

### Übergreifende Zielsetzungen nach innen:

- Steigerung von Effektivität und Effizienz bei der Leistungserbringung
- bessere Nutzung des Wissens und von Informationen

### Übergreifende Zielsetzungen nach außen:

- Beschleunigung und Steigerung der Entscheidungsqualität
- stärkere Dienstleistungs- und Kundenorientierung
- größere Transparenz und Nachvollziehbarkeit von Entscheidungen (**Sicherung des Informationszugangs**)
- Dialog- und Partizipationsmöglichkeiten (mehr **bürger-schaftliche Teilhabe**)

# Datenschutzgerechtes eGovernment



## Innenansicht eGovernment: Handlungsfelder

### Intranet

- „papierloses“ Büro
- Workflow
- Dokumenten-  
Management
- elektronische  
Archivierung
- Zahlungsverfahren
- Wissensmanagement

### Internet

- Kommunikation  
per eMail
- Web-Auftritt
- virtuelle Poststelle
- Online-Formulare
- Identifizierung/  
Authentifizierung

### Potentiale

### Gefahren

### Erwartungen

### Handreichung

### Handlungs- empfehlungen

### Ausblick

# Datenschutzgerechtes eGovernment



## Personenbezogene Daten im eGovernment

- Verarbeitung mit **gezielten Personenbezug** zum Zweck der personenbezogenen und personenbeziehbaren Verwendung (z.B. Bauakten, Vertragsdaten, Bestandsdaten)
- Verarbeitung **ohne gezielten Personenbezug** zu anderen Zwecken als dem Zweck der personenbezogenen und personenbeziehbaren Verwendung (z.B. Erbringung technischer Dienstleistung, Kommunikation von Maschine zu Maschine)

Potentiale

Gefahren

Erwartungen

Handreichung

Handlungs-  
empfehlungen

Ausblick



## Generelle Bedrohungen Bei elektronischer Informationsverarbeitung

- Unsichtbarkeit elektronischer Informationen
- Flüchtigkeit, spurenloser Verlust
- Aufhebung der räumlichen Anbindung
- mangelnde Nachvollziehbarkeit
- unbegrenzte Reproduzierbarkeit, kaum Unterscheidungsmöglichkeiten zwischen Original und Kopie bei elektronischen Dokumenten

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

**Potentiale**

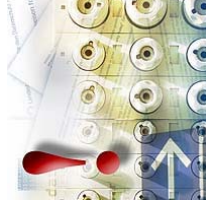
**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**



## Spezifische Bedrohungen (1)

- informationelle Gewaltenteilung und Zweckbindung können durchbrochen werden
- Verdichtung zu Persönlichkeitsprofilen
- Entscheidungsfindung wird automatisiert
- Nachvollziehbarkeit und Transparenz für Betroffene ist nicht gegeben

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**



## Spezifische Bedrohungen (2)

- Zunahme personenbezogener Daten (Bestands-, Nutzungs- und Verbindungsdaten)
- gesamte Kommunikation Einzelner mit der Behörde kann erfasst und analysiert werden
- Daten können zusammengeführt werden oder gezielt recherchiert werden (Datamining)



# Datenschutzgerechtes eGovernment

Potentiale
<b>Gefahren</b>
Erwartungen
Handreichung
Handlungs- empfehlungen
Ausblick

## Zielkonflikte mit Datenschutz

Erhebung beim Betroffenen	<b>versus</b>	Zugriff auf vorhandene Datenbestände
Zweckbindung	<b>versus</b>	Leistungsintegration
Abschottung	<b>versus</b>	one-stop-government/ multifunktionale Serviceläden
Transparenz	<b>versus</b>	Trennung von Produktion und Vertrieb, Front- Office/Back-Office
Vertraulichkeit	<b>versus</b>	Nutzung des Internet

# Datenschutzgerechtes eGovernment



## Einschätzungen national

### In Deutschland:

- **82%** halten die Nutzung des Internet beim eGovernment für unsicher
- davon die Hälfte sogar für „sehr unsicher“  
(TSM-Emnid 2002)

### In der Schweiz:

- **76 %** halten online Angebote des Staates nur ohne Preisgabe persönlicher Daten für sinnvoll
- **60%** befürchten, dass dem Staat zu viele persönliche Daten zugänglich werden  
(GfS-Forschungsinstitut 2003)

Potentiale

Gefahren

Erwartungen

Handreichung

Handlungs-  
empfehlungen

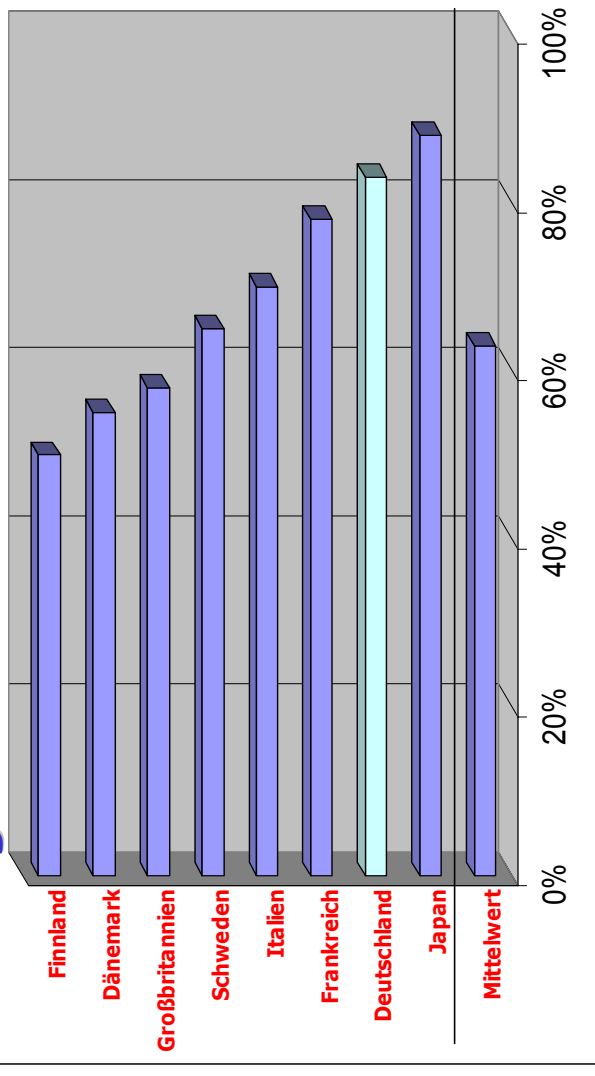
Ausblick



## Einschätzungen international

Potentiale  
Gefahren  
**Erwartungen**  
Handreichung  
Handlungs-  
empfehlungen  
Ausblick

Meinung „eGovernment ist unsicher“

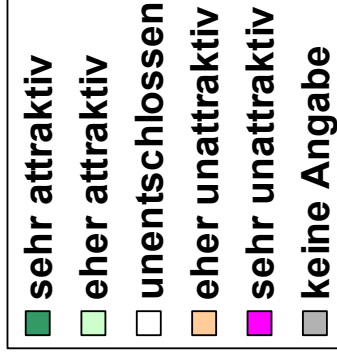
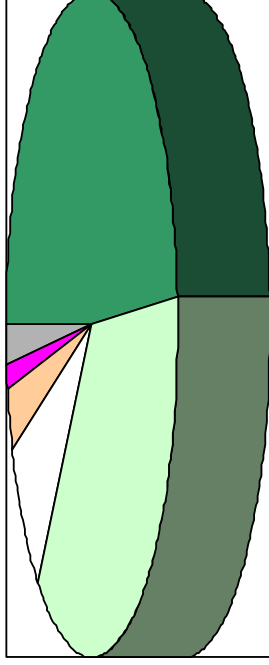


Quelle: TSN Emnid 2002

# Datenschutzgerechtes eGovernment

Potentiale  
Gefahren  
**Erwartungen**  
Handreichung  
Handlungs-  
empfehlungen  
Ausblick

## Bürger wollen eGovernment



Emnid/D21 2002

# Datenschutzgerechtes eGovernment

Potentiale

Gefahren

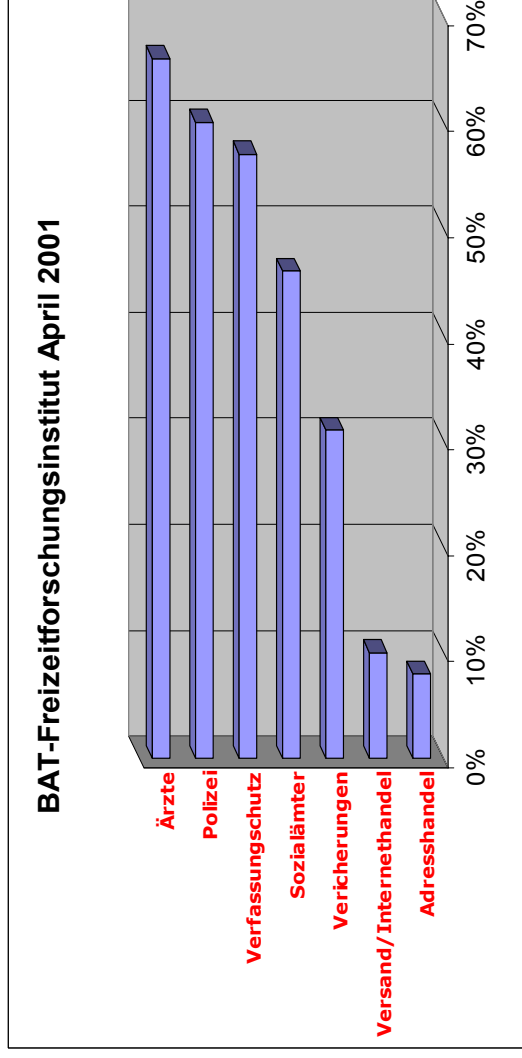
Erwartungen

Handreichung

Handlungs-  
empfehlungen

Ausblick

## Vertrauen in Institutionen



Vertrauensvorschuss beim Datenschutz in  
öffentliche Institutionen, der beim  
eGovernment nicht verspielt werden darf!

# Datenschutzgerechtes eGovernment



## Einschätzungen von Otto Schily

„Sichere und vertrauliche Kommunikation und datenschutzgerechte Lösungen sind **zwingende Voraussetzung** für die Akzeptanz des eGovernment bei den Nutzerinnen und Nutzern. Ohne diese Sicherheit werden die Menschen den neuen technischen Möglichkeiten **nicht vertrauen und sie auch nicht nutzen.**“

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

# Datenschutzgerechtes eGovernment

Potentiale
Gefahren
Erwartungen
<b>Handreichung</b>
Handlungs- empfehlungen
Ausblick



## Haltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

„Die Konferenz **unterstützt alle Bemühungen**, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen **schneller, einfacher, effektiver und insbesondere transparenter** zu machen. Die Datenschutzbeauftragten **erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.**“

(Entschließung vom 12./13. Oktober 2000)

# Datenschutzgerechtes eGovernment



## Haltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Potentiale

Gefahren

Erwartungen

**Handreichung**

Handlungs-  
empfehlungen

Ausblick

„Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern sowie ein angemessener Schutz der personenbezogenen Daten gewährleistet wird. Nur so ist die notwendige Akzeptanz auf Seiten der Bürgerinnen und Bürger sowie der anderen „Kunden“ der Verwaltung zu erreichen.“



# Datenschutzgerechtes eGovernment



**Arbeitsgruppe der DSB-  
Konferenz: Beteiligung  
aller LfD`s und des BfD**

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

**Ziel:** Erarbeitung einer Handreichung mit Darstellung der **Anforderungen** und unmittelbar umsetzbaren **Handlungsempfehlungen**, um eGovernment zum **raschen Durchbruch** zu verhelfen.

**Mitarbeiter:** BSI, Begleitforschung zu Media@Komm und die Professoren Roßnagel und Lenk

# Datenschutzgerechtes eGovernment



**Handreichung:  
Datenschutzgerechtes  
eGovernment**

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

## **Handlungsempfehlungen zur**

- Gewichtung personenbezogener Daten
- Erforderlichkeit und Verhältnismäßigkeit
- Datenvermeidung und Datensparsamkeit
- Einwilligung
- Sicherung der Zweckbindung
- Transparenz

# Datenschutzgerechtes eGovernment



**Datenschutzgerechtes  
eGovernment:**  
weitere anwendungsorientierte  
Handlungsempfehlungen zu

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

- Informationsangeboten
- eMail
- Identifizierungen
- Virtuelle Poststelle
- Grunddaten im virtuellen Schließfach
- Zahlungsverfahren
- Dokumentenmanagement
- Protokollierungen
- Einschaltung Dritter

# Datenschutzgerechtes eGovernment

## Forderung – eGovernment für jedermann!

- leistungsfähige, für alle zugängliche technische Infrastruktur (Geräte, Netze, Programme)
- Vermittlung technischer und kultureller Medienkompetenz
- Problemgruppen: ältere Menschen, sozial Schwache, Zuwanderer, Behinderte
- Erhaltung der kommunikativen Autonomie, Bereithalten analoger Handlungsmöglichkeiten
- Problem des „digital divide“

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

Potentiale
Gefahren
Erwartungen
Handreichung
<b>Handlungs- empfehlungen</b>
Ausblick



## Handlungsempfehlungen zur Datensparsamkeit und Datenvermeidung (I)

- Systeme und Anwendungen sind so zu gestalten, dass sie ohne personenbezogene Daten auskommen
- Anwendungen, bei denen eine persönliche Identifikation nicht zwingend erforderlich ist (z.B. reiner Info- oder Formularabruf), müssen auf die Abfrage personenbezogener Daten verzichten
- für statistische Auswertungen sollte nur eine gekürzte IP-Adresse erfasst werden



## Handlungsempfehlungen zur Datensparsamkeit und Datenvermeidung (II)

- soweit technisch möglich und zumutbar, ist eine anonyme oder pseudonyme Nutzung der Anwendung und Bezahlung zu ermöglichen (§ 4 Abs. 6 TDDSG)
- personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu löschen, zu anonymisieren oder zu pseudonymisieren
- bei eMail-Newslettern reicht die Erhebung der eMail-Adresse (nicht auch Name und postalische Anschrift)

Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick



## Handlungsempfehlungen zur Einwilligung (I)

- umfassende Aufklärung im Vorfeld über Umfang, Form und Zweck der Datenverarbeitung
- Hinweis auf Freiwilligkeit und Widerrufbarkeit
- kein „beiläufiges“ Abverlangen
- „opt-in“ Lösungen sollten gewählt werden
- Sonderproblem: Einwilligung in die Nutzung des elektronischen Weges erforderlich?

Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick

# Datenschutzgerechtes eGovernment



## Handlungsempfehlungen zur Einwilligung (II): Einwilligung in die Nutzung des elektronischen Weges?

§ 3 a VwVfG verlangt für die Übermittlung elektronischer Dokumente, dass „der Empfänger hierfür einen Zugang eröffnet“

- Reicht eMail-Adresse im Briefkopf?  
Bürgerinnen/Bürger: **nein**  
Firmen/Anwälte: ja
- reicht „Erstkommunikation“ per eMail?  
Bürgerinnen/Bürger: ja  
Firmen/Anwälte: ja

Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick



Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick



## Handlungsempfehlungen zur Protokollierung der Nutzung

- Protokoll Daten dürfen nur zu Zwecken genutzt werden, die Anlass für ihre Speicherung waren, und sind zum frühestmöglichen Zeitpunkt zu löschen
- Daten über die Inanspruchnahme verschiedener Online-Dienste müssen getrennt gespeichert werden
- bei kostenfreier Nutzung Löschung der Protokoll Daten nach Ende der Nutzung
- Verwendung von Protokoll Daten für Verhaltens- und Leistungskontrolle ist unzulässig

# Datenschutzgerechtes eGovernment

Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick



## Handlungsempfehlungen: Elektronische Zahlungsverfahren

- wenn im Verwaltungsverfahren keine Identifizierung erforderlich ist, sollte auch die Zahlung anonym oder pseudonym möglich sein
- Vertraulichkeit und Integrität der Daten müssen umfassend gewährleistet sein
- Zahlungsvorgänge müssen nachvollziehbar und das Sicherheitsniveau transparent sein
- für die Akzeptanz von elektronischen Zahlungssystemen hat die Einfachheit der Bedienung hohe Bedeutung

# Datenschutzgerechtes eGovernment

Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick



**Auf dem Weg zu einem  
datenschutzgerechten  
eGovernment – die  
Sicherungsziele!**

- **Vertraulichkeit** der übermittelten und gespeicherten Daten
- **Integrität** der übermittelten und gespeicherten Daten
- **Eindeutige Identifizierung** (Authentizität) des Betroffenen
- **Revisionsfähigkeit**

# Datenschutzgerechtes eGovernment

Potentiale

Gefahren

Erwartungen

Handreichung

**Handlungs-  
empfehlungen**

Ausblick



## Baukasten für technisch- organisatorische Werkzeuge

- Risikoanalyse und Vorabkontrolle
- Datensicherungskonzept
- Protokollierung
- Architekturmodell mit mehrstufiger Firewall/„demilitarisierte Zone“
- Nutzung von Verschlüsselungs- und Signaturkomponenten
- sichere Authentizität

# Datenschutzgerechtes eGovernment

Potentiale
Gefahren
Erwartungen
Handreichung
<b>Handlungs- empfehlungen</b>
Ausblick



## Musterlösungen und Referenzanwendungen

- Kapitel 7 der Handreichung enthält über 30 Praxisbeispiele von eGovernment-Anwendungen
- Anwendungen sind von der zuständigen Datenschutzaufsicht auf Datenschutz und Datensicherheit geprüft
- sie können als Lösungsansatz im Sinne von Referenz-Anwendungen empfohlen werden
- dadurch soll zugleich ein Beitrag zur Herausbildung von Standards geleistet werden



# Datenschutzgerechtes eGovernment

---

U N I K A S S E L  
V E R S I T Ä T

Prof. Dr. Alexander  
Roßnagel

Potentiale

Gefahren

Erwartungen

Handreichung

Handlungs-  
empfehlungen

Ausblick

„Datenschutz als Mittel zur Vertrauensgewinnung sollte als **Motor** zur Gestaltung und Nutzung von digitalisierten Behördenwegen dienen....Umso wichtiger ist es daher, den Datenschutz als **Wettbewerbsvorteil**, als **Beratungsgegenstand**, als **Dienstleistung**, als **Produktidee** und als **Aspekt der Selbstbestimmung** zu verstehen und zu gestalten.“

„Unzureichender Datenschutz kann beim Aufdecken illegitimer Datenverarbeitungen zur „**BSE-Krise**“ der **vernetzten Gesellschaft** werden.“



# Datenschutzgerechtes eGovernment

**Potentiale**

**Gefahren**

**Erwartungen**

**Handreichung**

**Handlungs-  
empfehlungen**

**Ausblick**

**Wichtige Arbeitshilfen**

**[www.lfd.niedersachsen.de](http://www.lfd.niedersachsen.de)**



# **Informationsfreiheit und Datenschutz Transparenz und eGovernment in Mittel und Osteuropa**

**Erfahrungen aus dem Projekt e-LoGo**



**A. Erhardt Ewert**

**Kommunalwissenschaftliches  
Institut der Universität Potsdam**

**Potsdam, den 10.11.2003**





## Das Projekt e-LoGo



- Projektförderung durch das Ministerium für Wissenschaft, Forschung und Kultur des Landes Brandenburg
- Laufzeit: 01.01.2001 - 31.12.2003
- angesiedelt am Kommunalwissenschaftlichen Institut der Universität Potsdam

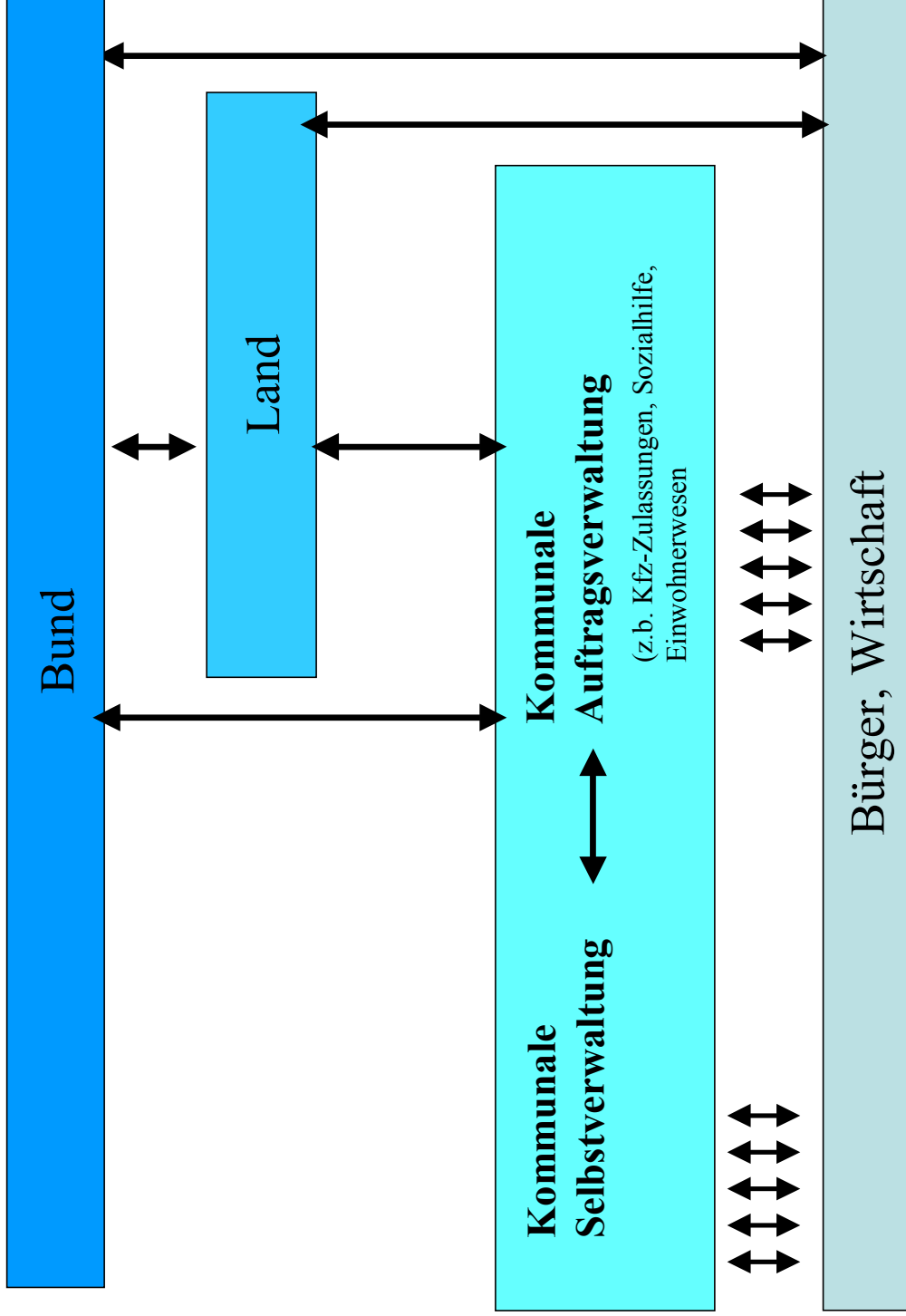
### **Projektleitung:**

- Herr Prof. Dr. Chr. Reichard (Projektleiter); Lehrstuhl Public Management
- Frau Prof. Dr. E. Horn; Lehrstuhl Software Engineering
- Herr Prof. Dr. D. Wagner; Lehrstuhl Organisation und Personal
- Herr Prof. Dr. W. Jann; Lehrstuhl Verwaltung und Organisation

### **Projektmitarbeiter:**

- A. Erhardt Ewert; Dipl. Politikwissenschaftler
- Thomas Off, Dipl. Informatiker
- Jörg Penning-Poggenbeck, Dipl.-Soziologe
- Tino Schuppan; Dipl. Verwaltungswissenschaftler

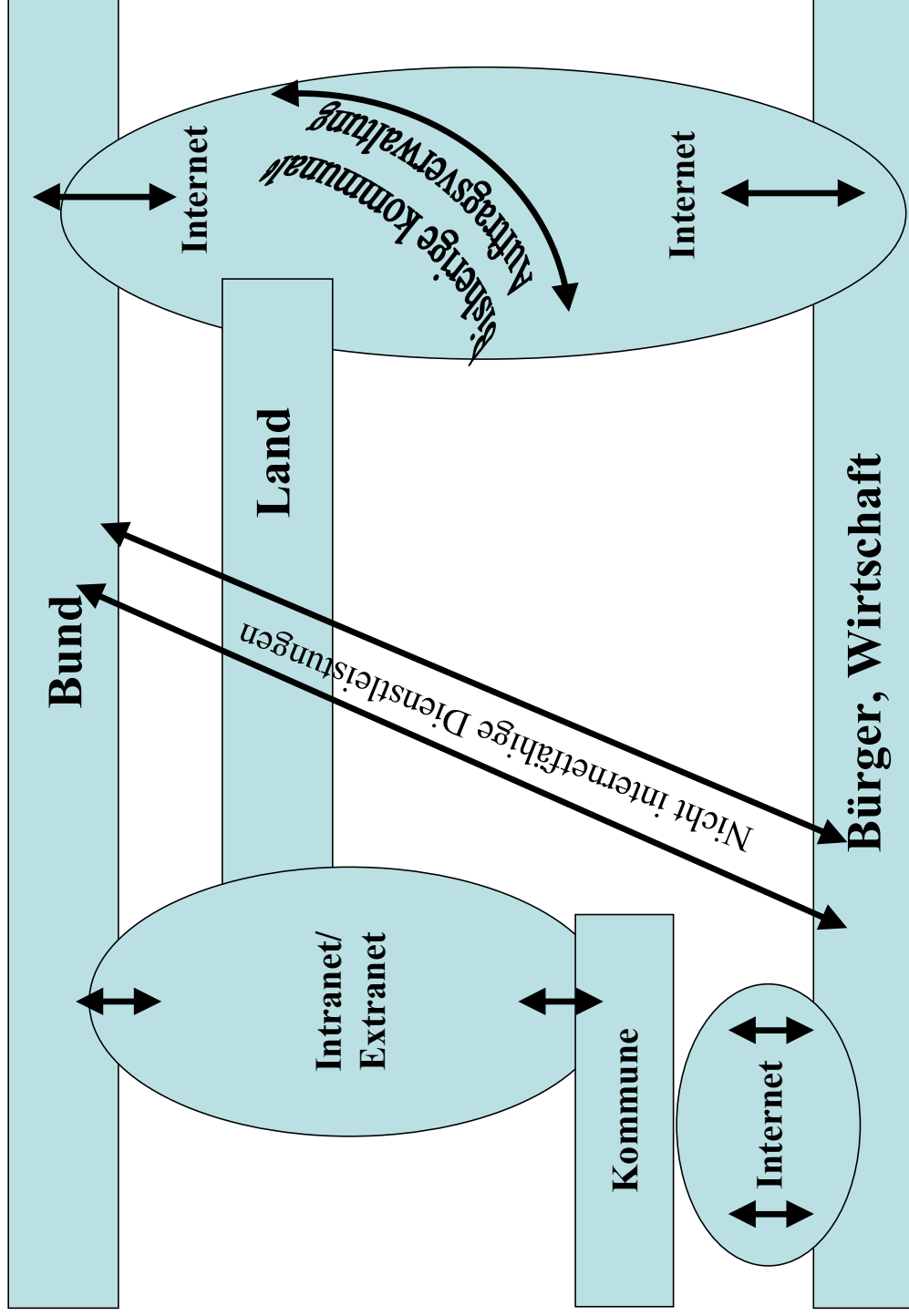
# Auftragsföderalismus



Einleitung

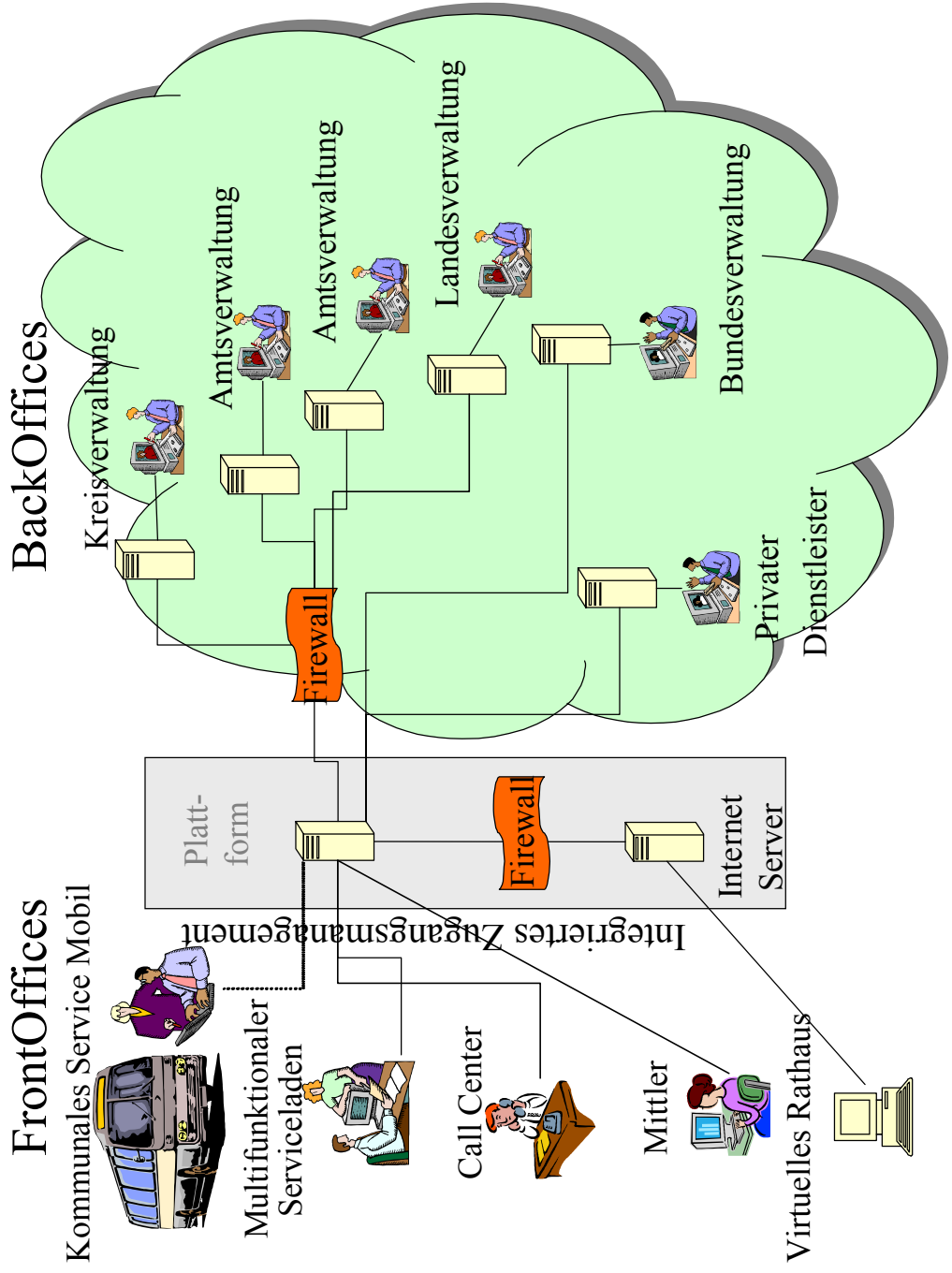
(Mehlich, 2002)

# Föderalistische Aspekte im Internet

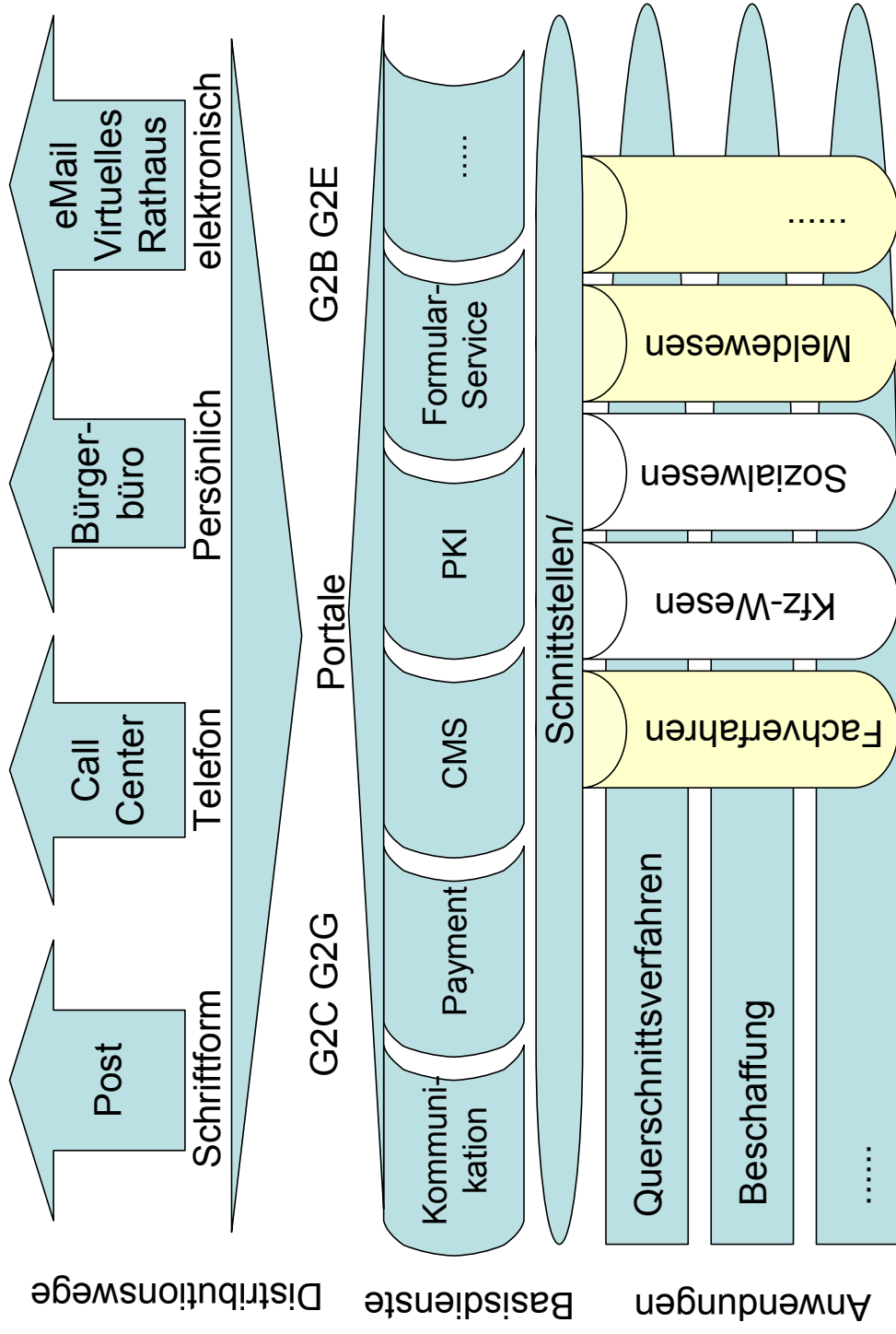


Einleitung

(Mehlich, 2002)



# eGovernment - Basisstruktur



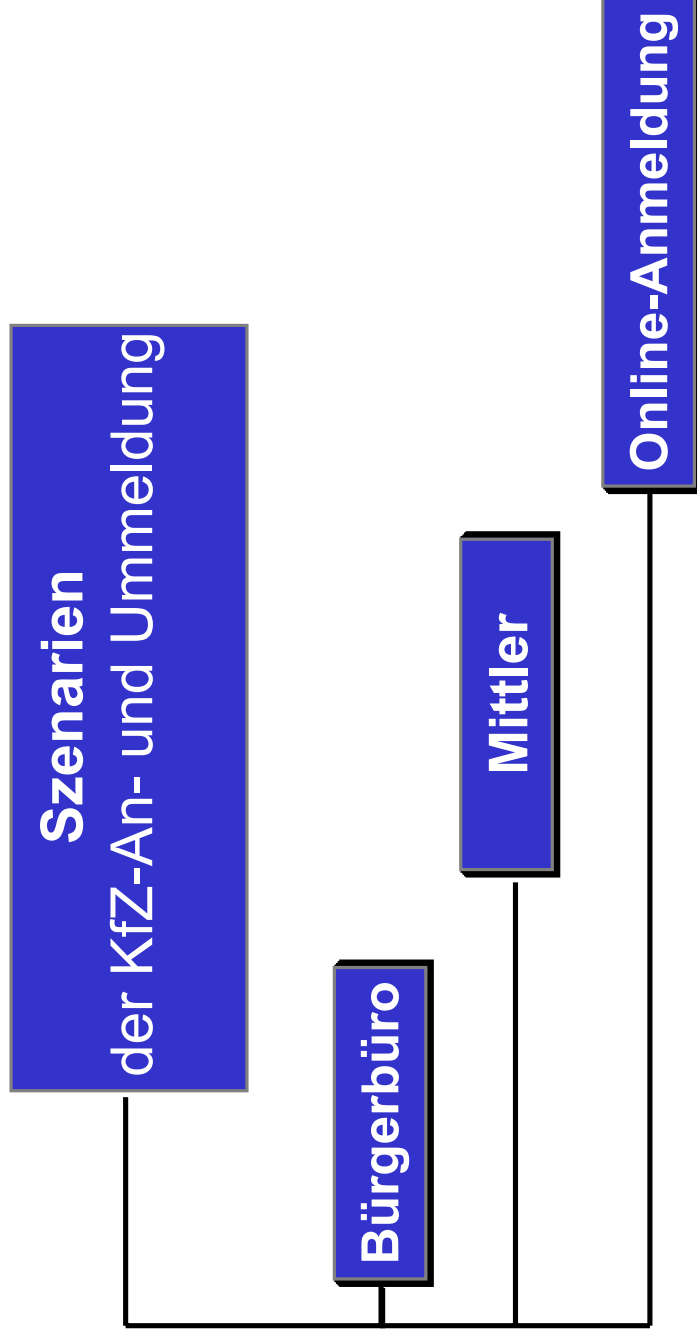
## Umfrage im Straßenverkehrsamt durchgeführt im November 2001



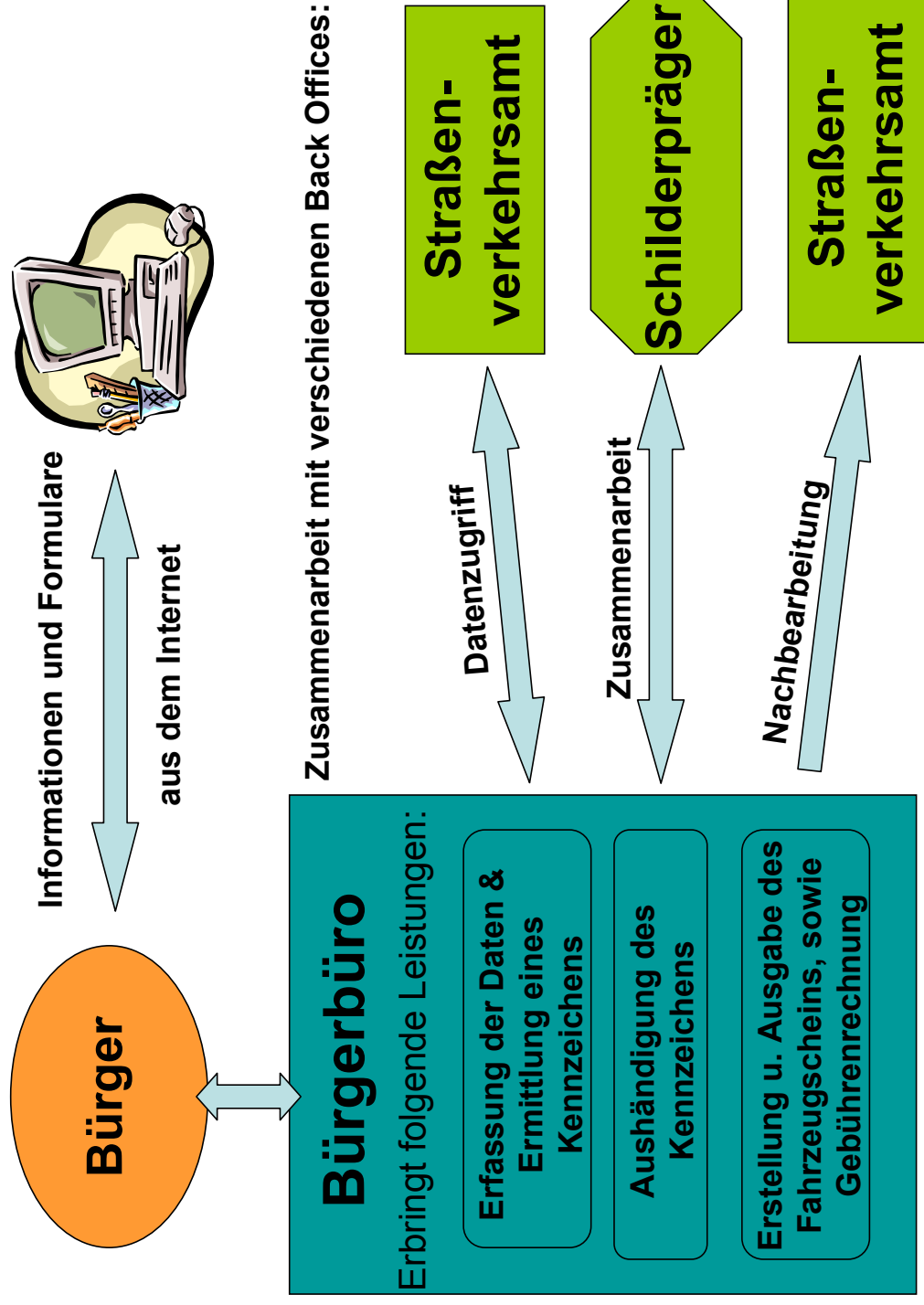
Wo würden Sie die Leistungen des Straßenverkehrsamtes bevorzugt in Anspruch nehmen?

Internet	Anzahl der Nennungen	Häuf.
Keine Angabe	18	2,1%
Zentral im Straßenverkehrsamt beim zuständigen Sachbearbeiter	137	16,3%
Ortsnah in Ihrem Amt/ Bürgerbüro bei einem allgemeinen Sachbearbeiter	395	46,9%
Vom heimischen PC über das Internet	292	34,7%
<b>GESAMT NENN.</b>	<b>842</b>	<b>100%</b>

## eGovernment-Szenarien



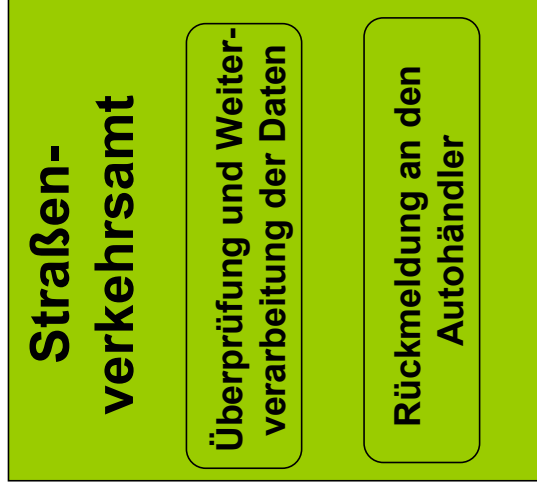
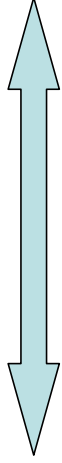
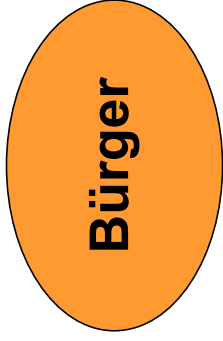
# Szenario 1: Ummeldung im Bürgerbüro



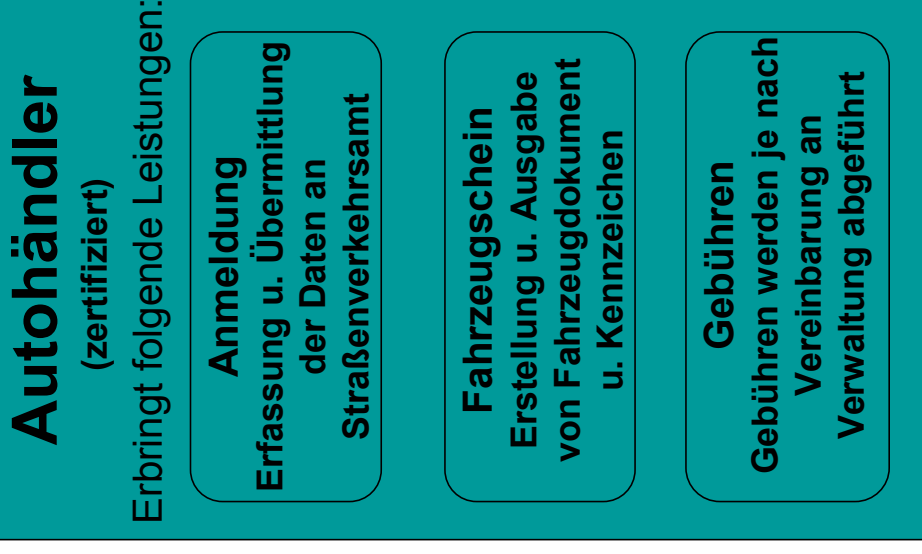
Straßenverkehrsamt



## Szenario 2: Anmeldung durch einen Autohändler

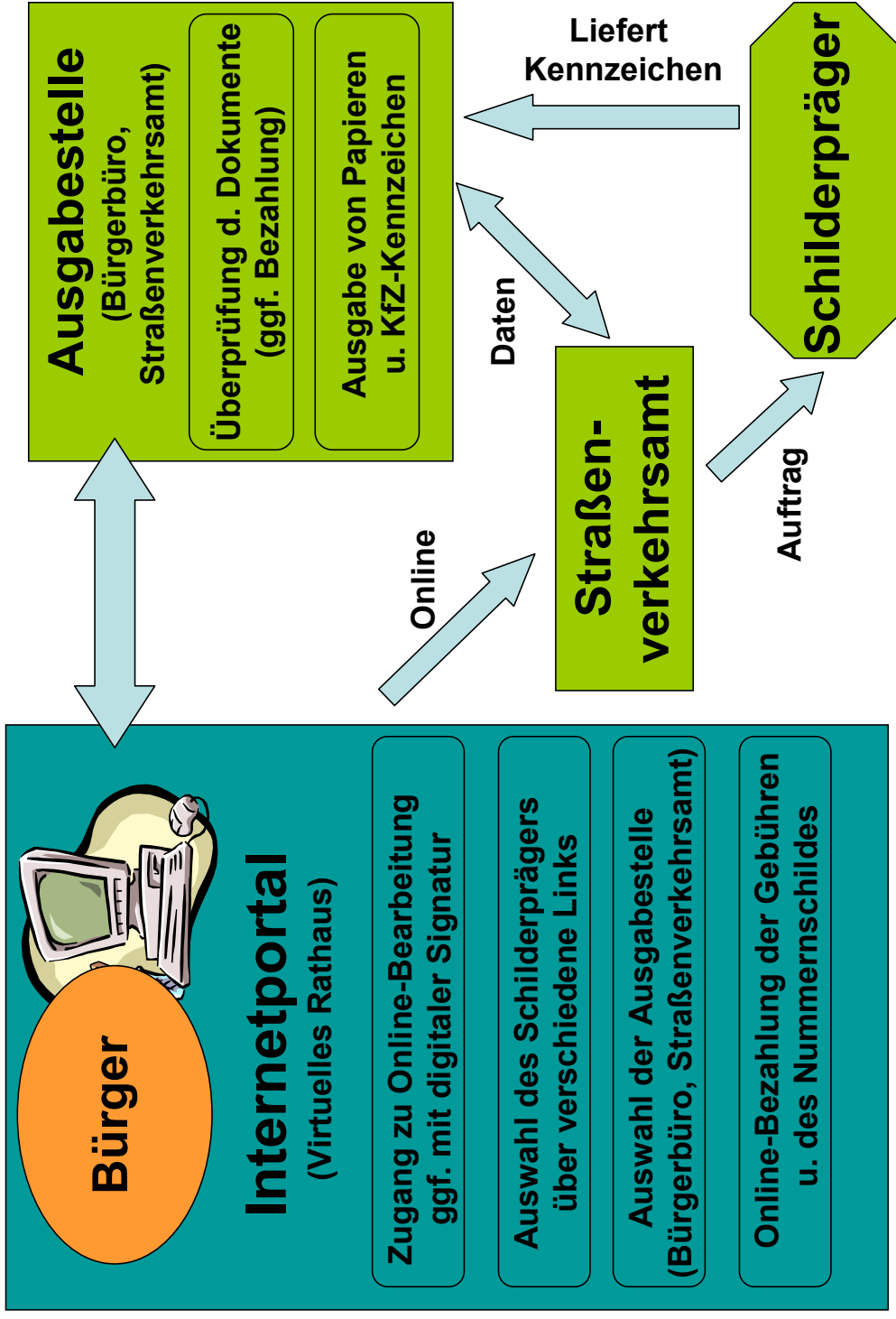


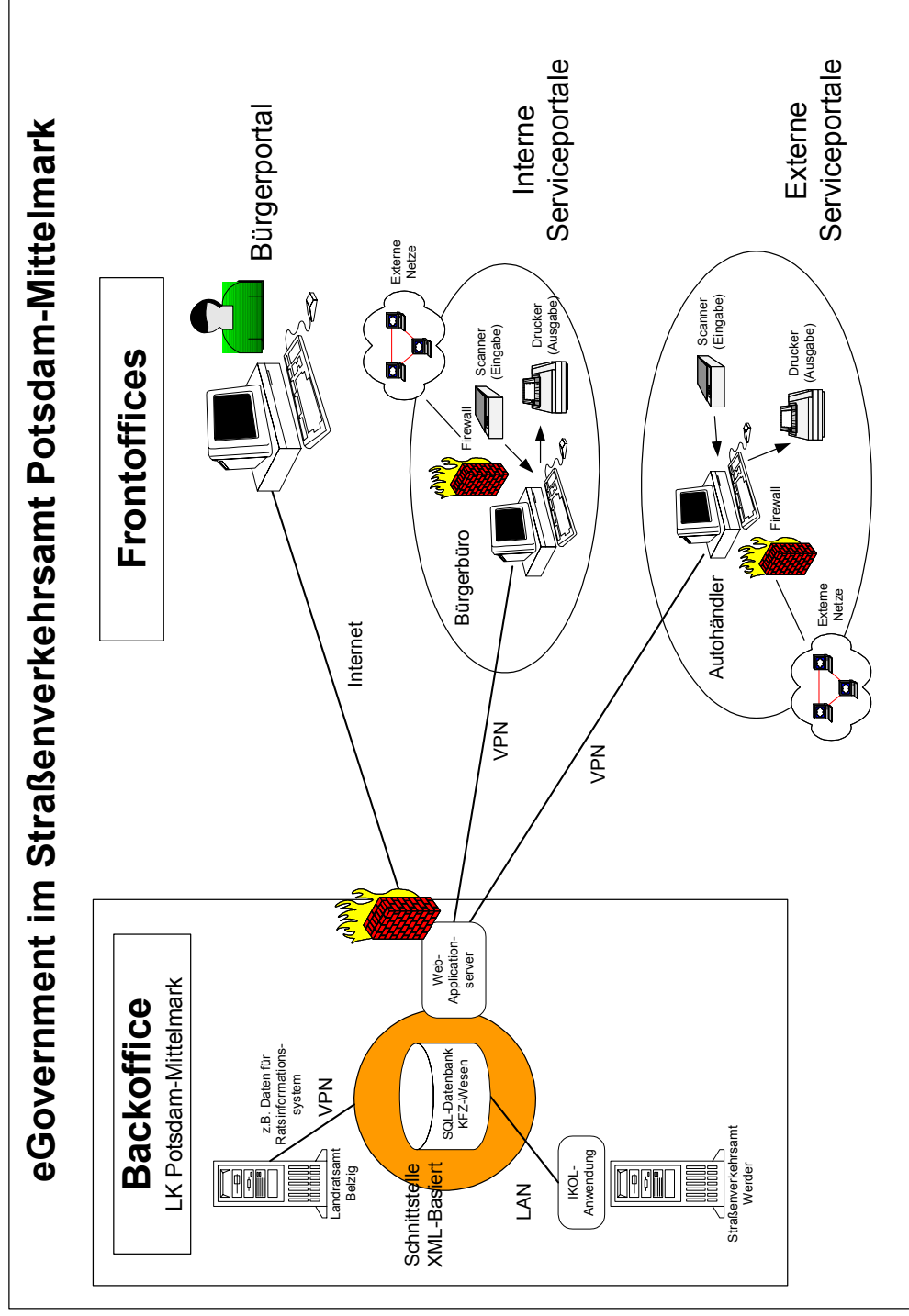
Interaktion über das Internet



Straßenverkehrsamt

# Szenario 3: KfZ-Online-Anmeldung





## Kfz-Ummeldung in Beelitz



Seit 2. Dezember 2002 im Einwohnermeldeamt möglich

- Halterwechsel innerhalb des Landkreises Potsdam-Mittelmark
- technische Änderungen & Änderungen von Angaben zum Fahrzeughalter
- Ausfertigung eines Ersatzfahrzeugscheines nach Verlust oder Diebstahl
- vorübergehende Stilllegung und endgültige Abmeldung
- Reservierung von Kennzeichen
- Anmeldung eines vorübergehend stillgelegten Fahrzeuges auf den gleichen Fahrzeughalter
- Zweitschrift einer Abmeldebescheinigung
- vorübergehende und endgültige Abmeldung von Fahrzeugen aus einem anderen Zulassungsbereich

Bereits an den ersten drei geöffneten Tagen, nahmen 29 Bürger die neue Dienstleistung in Anspruch. Der Schwerpunkt liegt dabei in der Halteränderung mit 18 Vorgängen, gefolgt von 6 vorübergehenden Stilllegungen, 3 Halterwechseln sowie jeweils einer Wiederanmeldung und Reservierung von Kennzeichen.

# Sozialwesen



**Back-Office A:  
Sozialamt**

Leistungen des  
Sozialamtes

**Back-Office B:  
Jugendamt**

Leistungen des  
Jugendamtes

**Front-Office:  
Bürgerbüro /  
Sozialbürgerhaus**

Dezentraler Bürgerservice



Digitale Integration  
der Leistungen  
externer Partner

**Arbeitsamt**

**Krankenkassen**

**Private Träger**

# Sozialwesen

# Sozialwesen



## Sozialamt

- Hilfe zum Lebensunterhalt nach BSGH
- Hilfe in besonderen Lebenslagen
- Leistungen nach Landesaufnahmegesetz und Asylbewerberleistungsgesetz
- Betreuungsangelegenheiten
- Versicherungsangelegenheiten
- Hilfe zur Unterhaltssicherung
- Berufsausbildungsförderung
- Blindenhilfe, Eingliederungshilfe, Pflegegeldanträge
- Rentenanträge
- Auskunftserteilung in  
Sozialversicherungsangelegenheiten

## Jugendamt

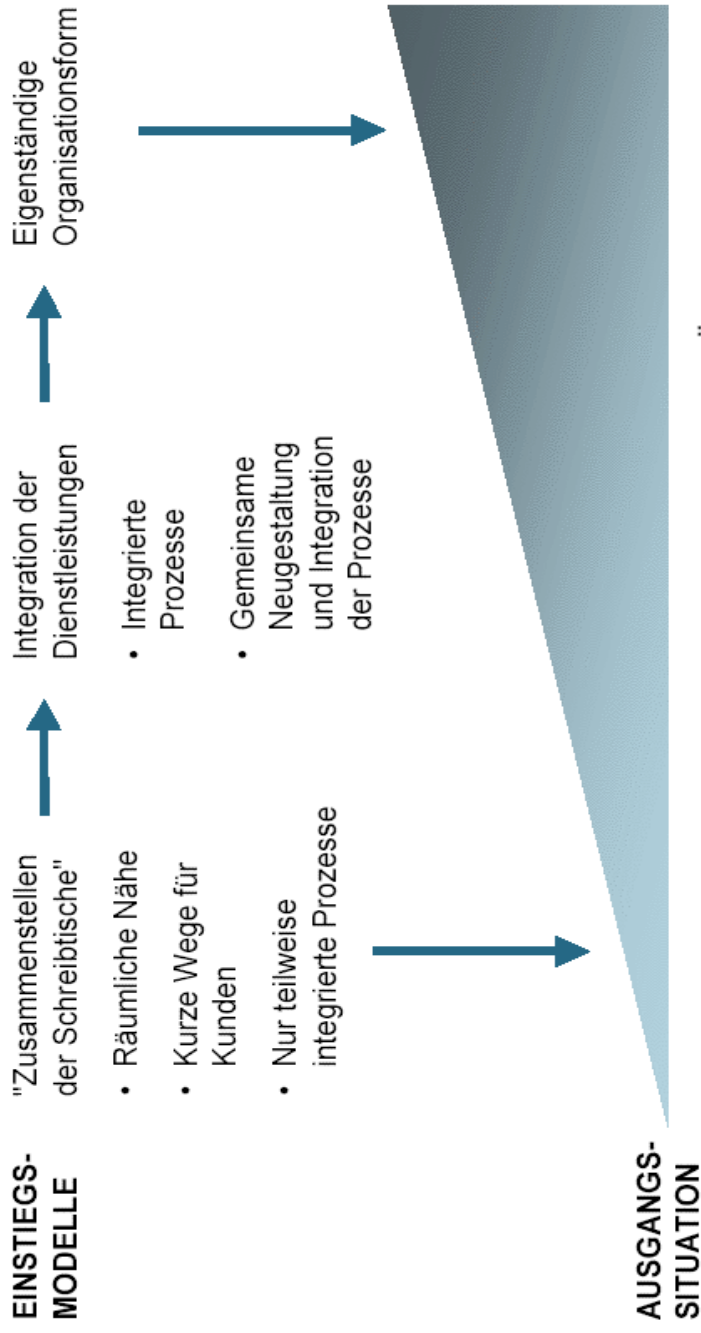
- Beratung und Hilfe für Kinder
- Beratung und Hilfe für Eltern
- Beratungs- und Therapiegespräche
- Führung von Vormundhaften/Pflegeschaften
- Unterhaltsüberprüfung / Neuberechnung
- Vaterschaftsanerkennung und Beurkundung von Unterhalt
- Unterhaltsvorschuss für Kinder
- Bundeserziehungsgeld
- Erstattung / Übernahme von Kita-Gebühren

Sozialbürgerhaus

Arbeitsamt

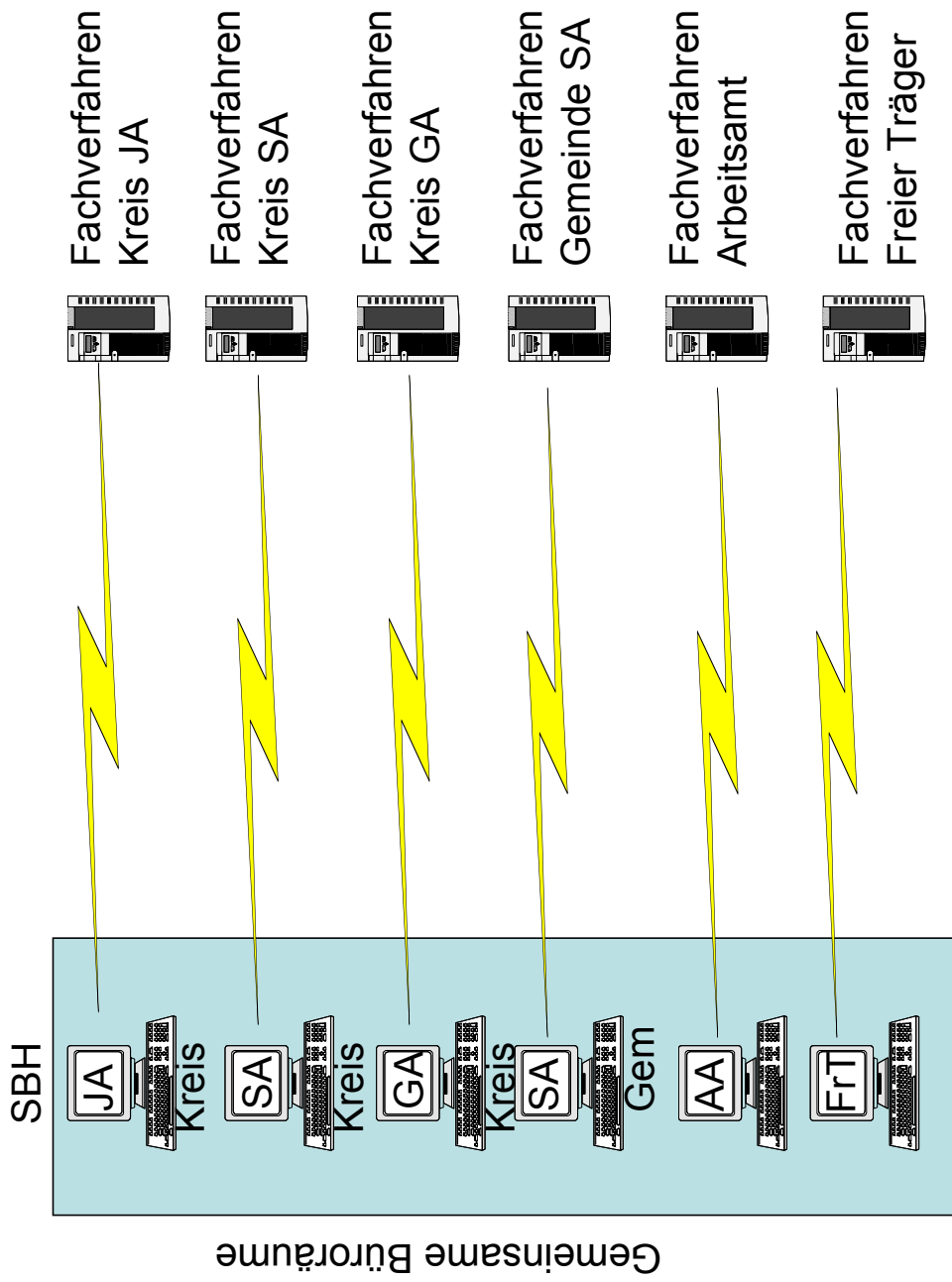
Private Träger

Krankenkassen



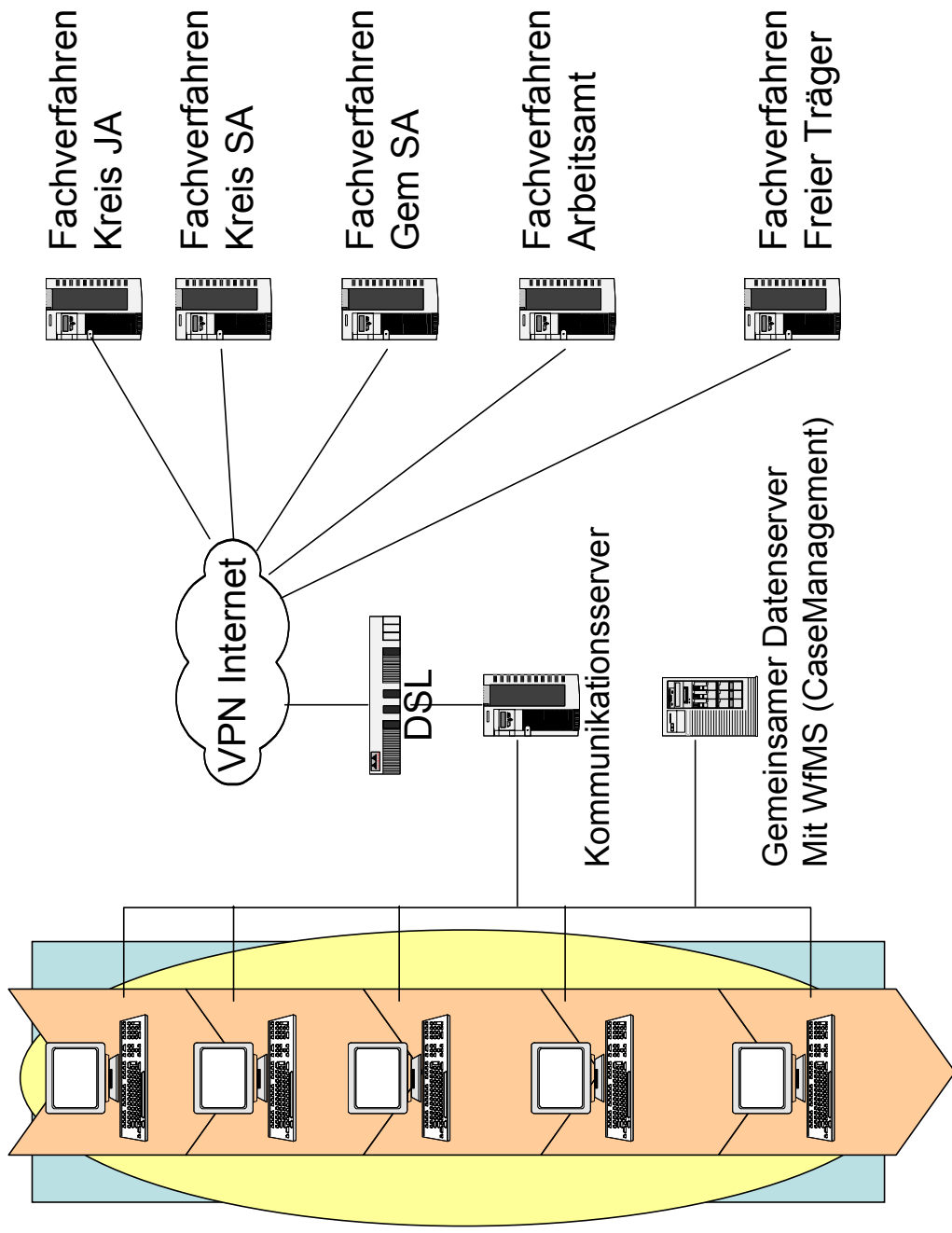
**INTENSITÄT DER KOOPERATION  
ZWISCHEN BA UND KOMMUNE**

# Technik SBH - Ist





# Technik SBH - Vision



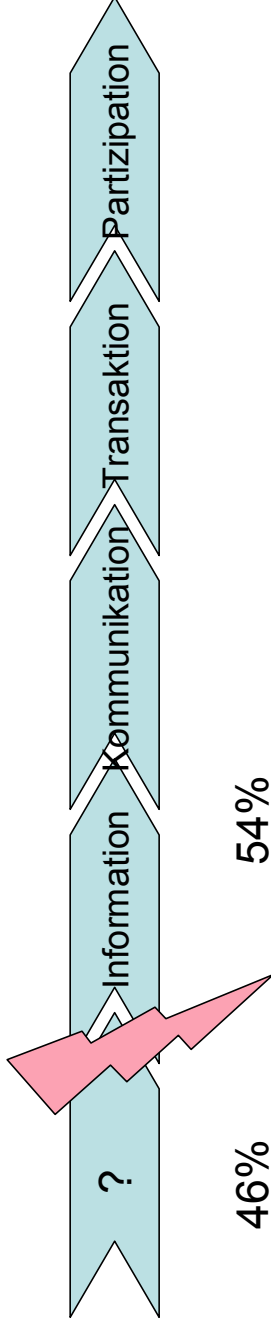
Sozialwesen

# Brandenburger Kommunen im Netz



Kommunalstruktur	Anzahl Kommunen	Anzahl der Internetseiten				
<b>nach Verwaltungseinheiten (Kommunalverwaltungen)</b>						
Landkreise	14	5,9%	1	3,0%	14	11,0%
kreisfreien Städte	4	1,7%	-	0,0%	4	3,1%
Ämter	135	57,0%	11	33,3%	55	43,3%
amtsfreie Städte	52	21,9%	17	51,5%	36	28,3%
amtsfreie Gemeinden	32	13,5%	4	12,1%	18	14,2%
Summe	237	100,0%	33	100,0%	127	100,0%

**100%**  
**100%**  
**41%**  
**69%**  
**56%**  
**54%**



## Web-Check

Datenquelle: Ministerium des Innern Bbg: „Online Kommunen“ unter [www.brandenburg.de](http://www.brandenburg.de), Stand 2002, Penning-Poggenbeck, J./ Scheske, M.

## Definition von Formularen



- 1 Bearbeitungsraster, die zweckmäßig gestaltet sind und einen einheitlichen Aufbau haben
- 2 enthalten wiederkehrende Informationen
- 3 am Anfang und am Ende eines Verwaltungsprozesses, oder treten im Verlauf des Vorganges hinzu
- 4 sind Erfassungsbögen bzw. –masken, die individuelle Daten für administrative Bearbeitungsprozesse in normierter Form sammeln bzw. die entsprechenden Daten nach Abschluss eines Bearbeitungsverfahrens an einen Empfänger übermitteln.

Formularservice

Aufgrund ihrer zentralen Rolle im Verwaltungsverfahren sind sie der ideale Einstiegspunkt für Prozessdigitalisierung.

# Online-Formulare in Brandenburg



Kriterium	Ausprägung	Landkreise		Amtsfreie Gemeinden		Kreisfreie Städte		Ämter		Amtsfreie Städte	
		N	%	N	%	N	%	N	%	N	%
<b>Download-Dokumente</b>	umfangreich vorhanden	5	35,7%	11	61,1%	1	25,0%	4	7,3%	4	11,1%
	vorhanden	6	42,9%	1	5,6%	0	0,0%	22	40,0%	15	41,7%
	nicht vorhanden	3	21,4%	6	33,3%	3	75,0%	29	52,7%	17	47,2%
	gesamt	14	100,0%	18	100,0%	4	100,0%	55	100,0%	36	100,0%
<b>Download-Formulare</b>	umfangreich vorhanden	2	14,3%	6	33,3%	1	25,0%	1	1,8%	4	11,1%
	vorhanden	4	28,6%	2	11,1%	0	0,0%	15	27,3%	5	13,9%
	nicht vorhanden	8	57,1%	10	55,6%	3	75,0%	39	70,9%	27	75,0%
	gesamt	14	100,0%	18	100,0%	4	100,0%	55	100,0%	36	100,0%
<b>Online-Formulare</b>	umfangreich vorhanden	0	0,0%	0	0,0%	0	0,0%	0	0,0%	0	0,0%
	vorhanden	1	7,1%	0	0,0%	0	0,0%	1	1,8%	1	2,8%
	nicht vorhanden	13	92,9%	18	100,0%	4	100,0%	54	98,2%	35	97,2%
	gesamt	14	100,0%	18	100,0%	4	100,0%	55	100,0%	36	100,0%

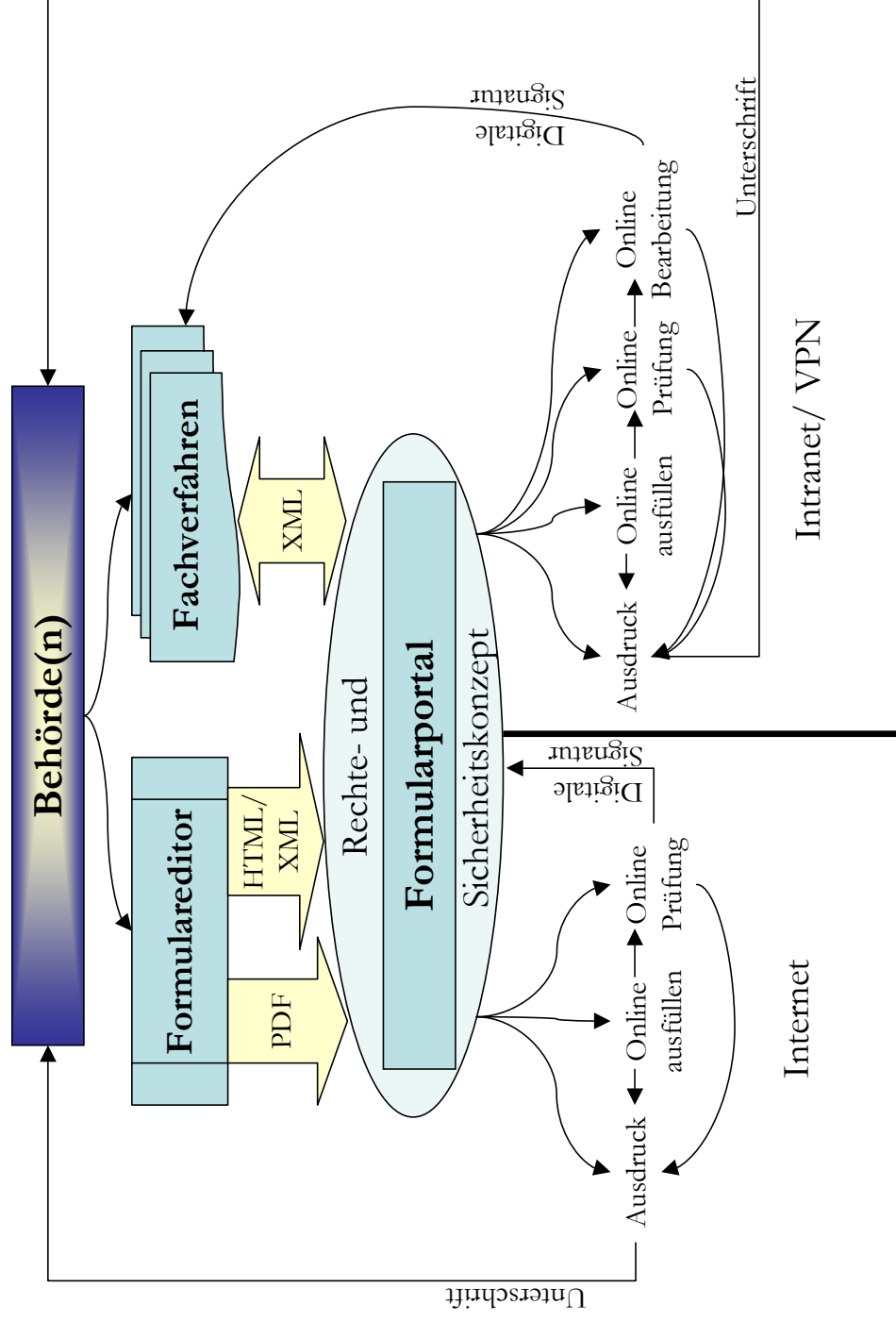
## Formulare in der Kreisverwaltung

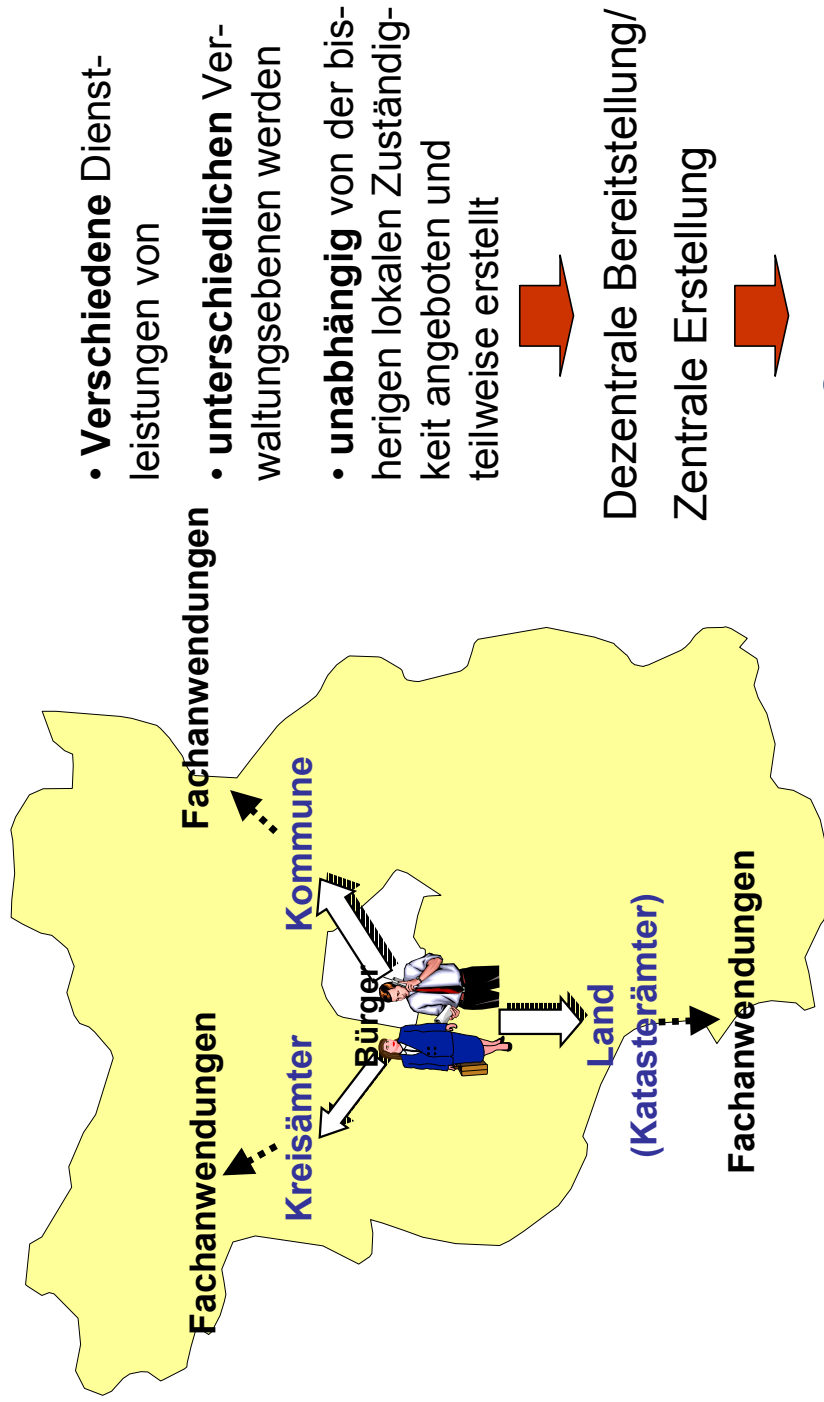


- ↑ Insgesamt mehr als 600 Formulare
- ↑ Heterogene Bezugskanäle
- ↑ 50% bereits in digitaler Form vorhanden, aber unterschiedliche Formate
- ↑ z.T. schon hohe Nutzung von Downloadformularen
- ↑ Erheblicher Verwaltungsaufwand

1. Kreiseigenes Formularportal
2. Kooperatives Formularportal
3. Landesformularportal
4. Länderübergreifendes Formularportal

Formularportale müssen neben der „Formular“-Bereitstellung u.a. auch Signatur-, Payment-, HelpDesk- Funktionalität integrieren.





- **Verschiedene** Dienstleistungen von
- **unterschiedlichen** Verwaltungsebenen werden
- **unabhängig** von der bisherigen lokalen Zuständigkeit angeboten und teilweise erstellt



Dezentrale Bereitstellung/  
Zentrale Erstellung



**One stop  
Government**

Ausblick

↑  
Neue Form von interkommunalem Wettbewerb?





Die technische Revolution in Berlins Amtsstuben

## Für weitergehende Informationen:

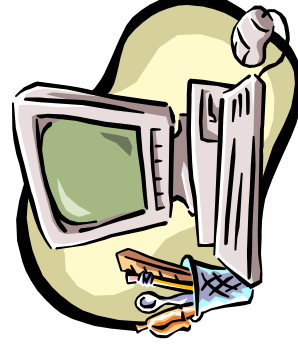


Universität Potsdam  
Kommunalwissenschaftliches Institut  
Projekt e-LoGo  
Am Park Babelsberg 14  
14482 Potsdam



0331/ 977 – 4505 (T. Schuppen/ T. Off)  
0331/ 977 – 4470 (A.E. Ewert)  
0331/ 977-4434 (J. Penning-Poggenbeck)  
Fax: 0331/ 977 – 4613

aeewert@rz.uni-potsdam.de  
penning@rz.uni-potsdam.de  
schuppen@rz.uni-potsdam.de  
thomoff@rz.uni-potsdam.de



[www.e-lo-go.de](http://www.e-lo-go.de)



---

# Identitätsmanagement und E-Health

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz  
Schleswig-Holstein, Deutschland

10. November 2003, Potsdam



UNABHÄNGIGES LANDESZENTRUM  
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

---

*Identitätsmanagement und E-Health*



## Identitätsmanagement & E-Health: Eine Vision 1/2

*Silvia has an accident. Hopefully nothing serious, but to be on the safe side, she wants to see a doctor.*

*When registering in the hospital, she shows her **health insurance certificate** which is stored on her PDA – it ensures that the hospital's bill will be paid, but does not contain her name: all patients can remain **anonymous** if they like to. Silvia is lucky: the doctor tells her that everything is alright; he only stores a **prescription** for the sedative Valerian on her PDA and recommends one message session.*

*She buys the sedative at the GetWell Inc. pharmacy, showing her prescription – again **without a reference to her real name** or address. The pharmacy signs the purchase so that she can get **refunding** from her **health insurance** by showing this certificate. Together with the Valerian she receives a **50%-off voucher** for the book "Herbs & Health", again stored on her PDA.*

*On the way home, she connects to her favourite Internet bookshop. (In the morning she has already been surfing its web site: Then she had logged in under her **regular customer profile** and was recommended the new book by her favourite science fiction author. She had immediately bought it and downloaded the text on her e-book, hoping to start reading it tonight.)*



## Identitätsmanagement & E-Health: Eine Vision 2/2

Now, when connecting to the web site again, her **browser's privacy window** signals her that the site's privacy policy is compliant with legal requirements as well as with Silvia's own privacy preferences.

Her browser informs her that the site already has her real name and PO box from previous interactions, but that she can choose to remain anonymous during this interaction: her **voucher** is an **anonymous** one; and the **communication channel** used by her browser is **by default anonymous**. She anonymously redeems the voucher, paying with **AnonCash**, and downloads the book on herbs.

Afterwards she surfs to the web site of RelaxNow, a massage salon. She fills in a **one-time phone number**, obtained by her PDA from her telco provider, where RelaxNow can reach her to make an appointment.

A few minutes later her PDA signals the incoming call, displaying who is calling, for which purpose, and the **massage therapist certificate** issued by the therapist organisation. They make an appointment for the evening.

Now she has time to calm down and read her new books.



# Überblick



- **Identitätsmanagement:**  
Nutzergesteuerter Datenschutz
- **Beispiele aus Praxis und Forschung:**  
Password Manager, Single Sign-On, Form Filler ...
- **Konzepte für nutzergesteuertes Identitätsmanagement:**  
Mit Pseudonymen, Credentials, History-Funktion, 3<sup>rd</sup> Parties
- **Identitätsmanagement im Bereich E-Health:**  
Rollen, Verfahren, Szenarien
- **Fazit und Ausblick**



## **Recht auf informationelle Selbstbestimmung**

***Jeder hat das Recht zu wissen,  
wer was über einen weiß.***

- **Motivation für Identitätsmanagement**
- **Grundsätzliche Wahl für jede(n),**
  - wem man was über sich erzählt und
  - wem gegenüber man wie auftritt
- **Identitätsmanagement in Nutzerhand:**
  - Steuerungsmöglichkeit
  - Transparenz

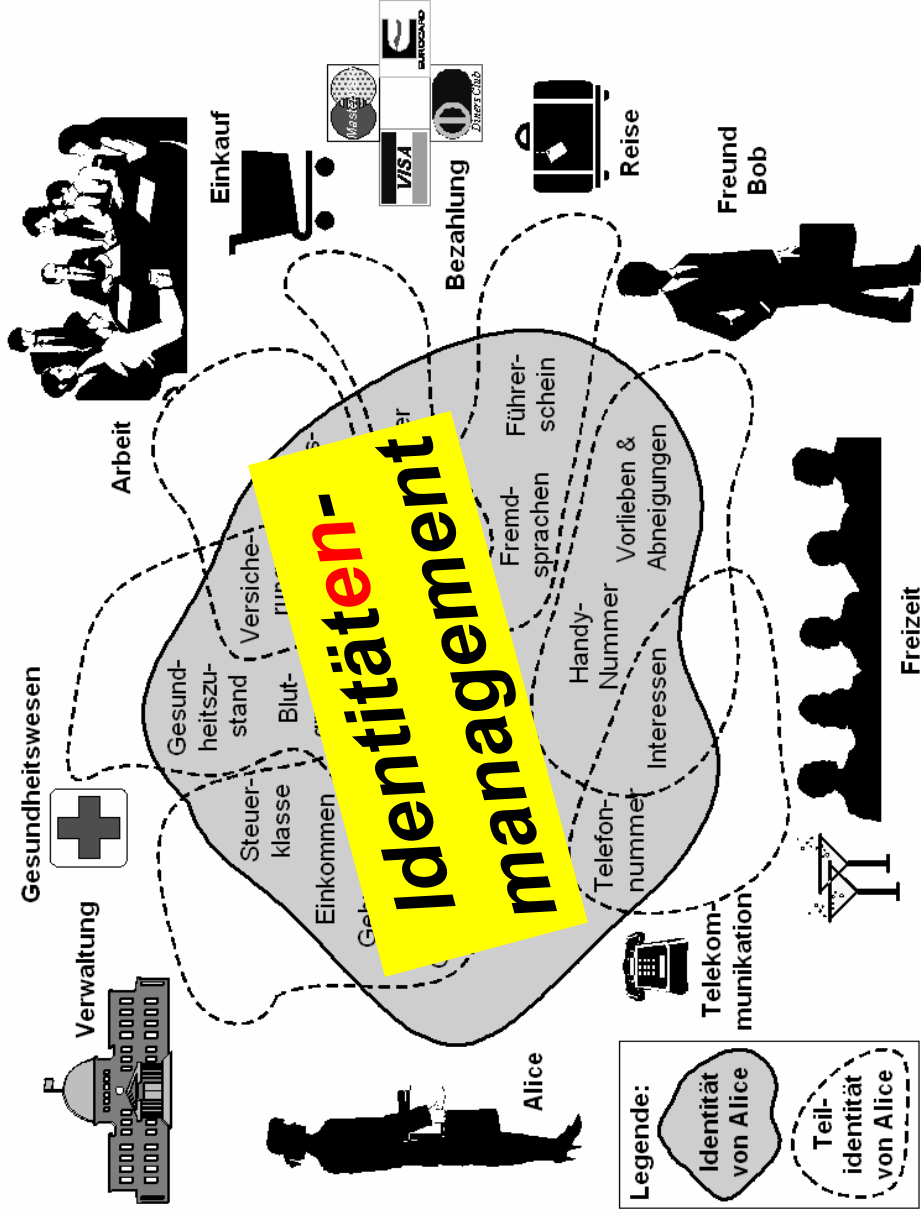
### **Heutiges digitales Leben:**

- **Profile durch Verkettung**
- **Identity Theft möglich**

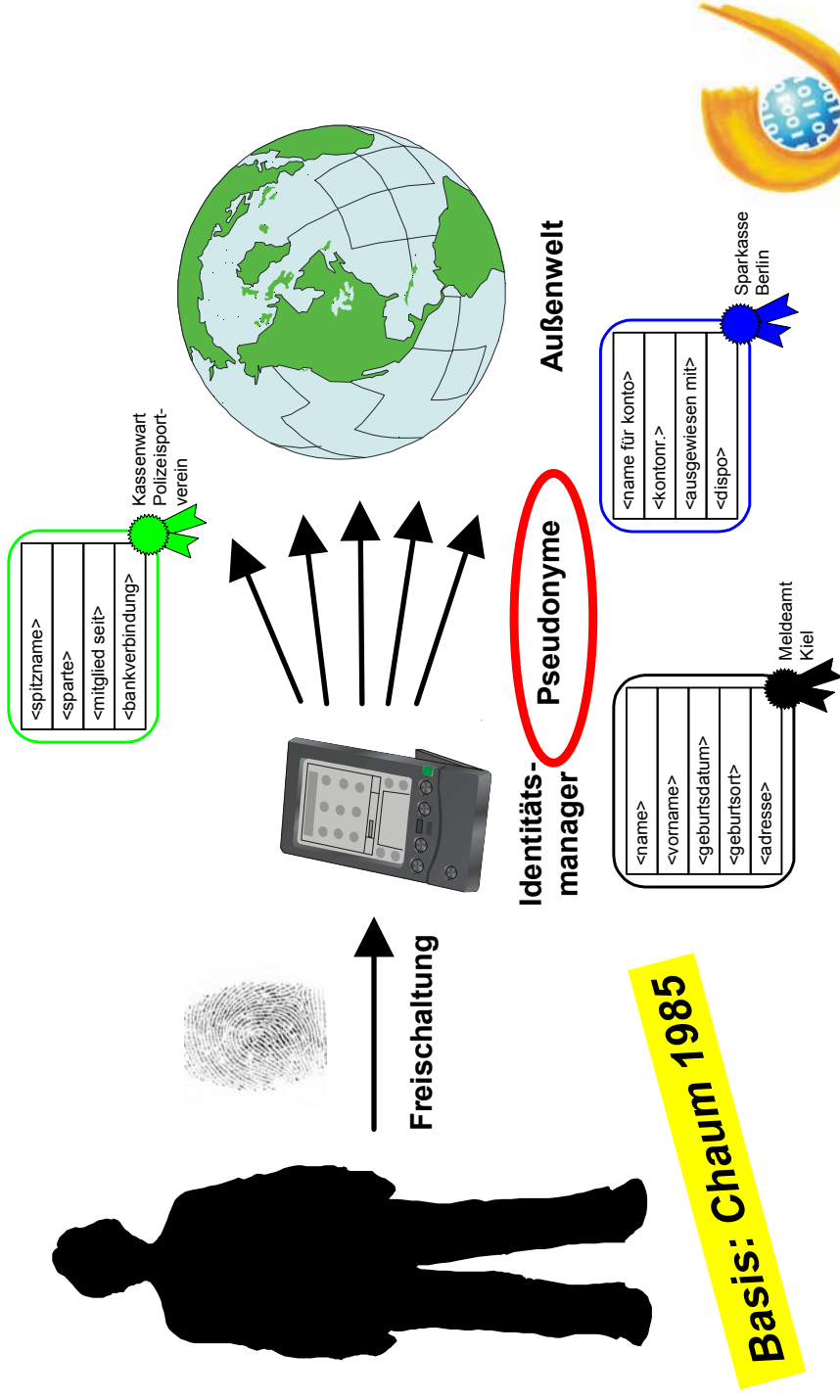




# Teilidentitäten von Alice



# Identitätsmanagement: Datenschutz in Nutzerhand



## Einsatzbereiche für Identitätsmanagement

- Komfortables Verwalten vorhandener Identitäten (insb. Single Sign-On, Form Filler)
- Authentikation und Zugriffskontrolle (inkl. dig. Signatur)
- Rollenmanagement, insb. Trennung von Berufs- und Privatleben
- Erreichbarkeitsmanagement
- Recht auf informationelle Selbstbestimmung: Balance von Anonymität und Authentizität bzw. Zurechenbarkeit



# Überblick

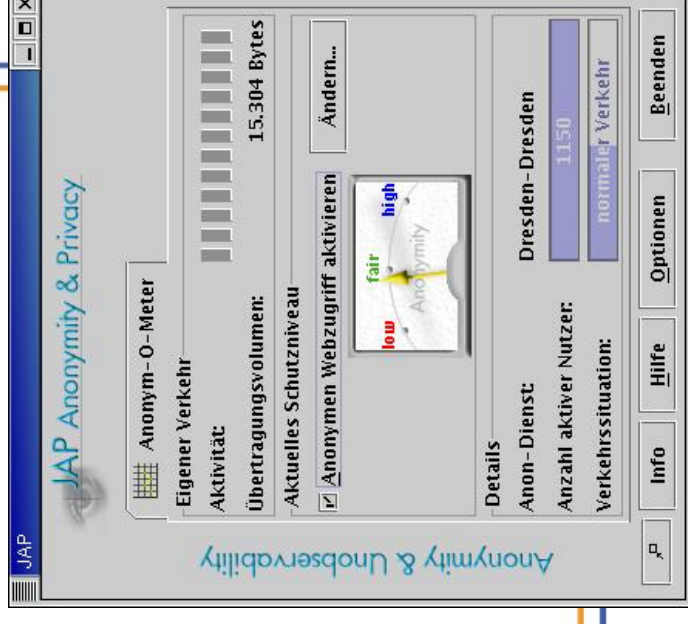


- **Identitätsmanagement:**  
Nutzergesteuerter Datenschutz
- **Beispiele aus Praxis und Forschung:**  
Password Manager, Single Sign-On, Form Filler ...
- **Konzepte für nutzergesteuertes Identitätsmanagement:**  
Mit Pseudonymen, Credentials, History-Funktion, 3<sup>rd</sup> Parties
- **Identitätsmanagement im Bereich E-Health:**  
Rollen, Verfahren, Szenarien
- **Fazit und Ausblick**

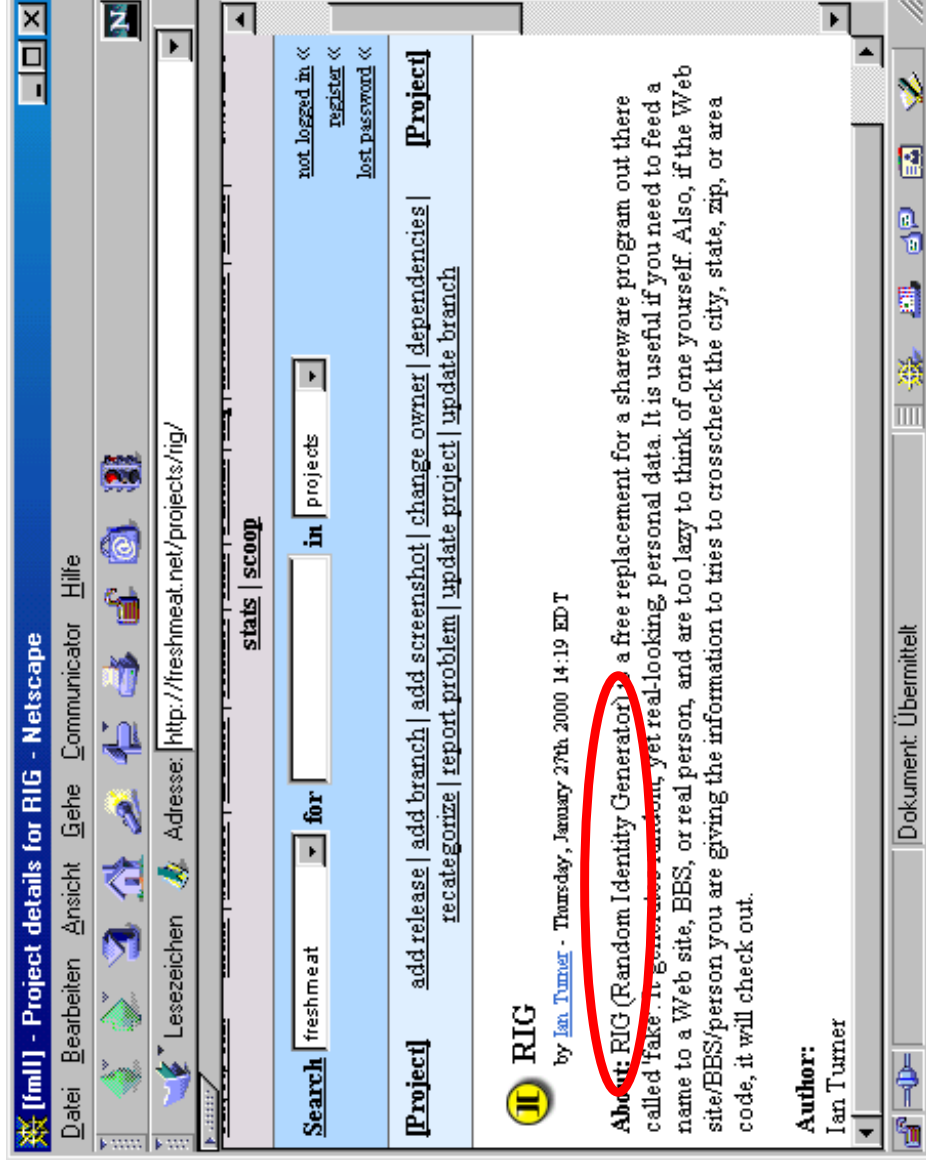


## Überblick: Identitätsmanagement aus Nutzersicht

- „manuell“
- Verwaltung von E-Mail-Accounts
- History-Funktionen
- spezielle Services mit Teilfunktionalität
- Einsatz von Identitätsmanagement-Prototypen
- ...
- **Begleitend: Tools für**
  - Verschlüsselung
  - Transparenz, z.B. P3P ([w3c.org/P3P/](http://w3c.org/P3P/))
  - Anonymität, z.B. AN.ON (<http://www.anon-online.de>)



# Form Filler „RIG - Random Identity Generator“



The screenshot shows the Netscape browser window titled "[fml] - Project details for RIG - Netscape". The address bar contains "http://freshmeat.net/projects/rig/". The main content area features a search bar with "freshmeat" entered, a "for" dropdown menu, and a "projects" dropdown menu. Below this is a navigation menu with links: "add release", "add branch", "add screenshot", "change owner", "dependencies", "recategorize", "report problem", "update project", and "update branch". A "Project" section is visible with links for "not logged in", "register", and "lost password". The main text area contains the following information:

**RIG**  
by [Ian Turner](#) - Thursday, January 27th 2000 14:19 EDT

**About:** RIG (Random Identity Generator) is a free replacement for a shareware program out there called 'fake'. It generates random, yet real-looking, personal data. It is useful if you need to feed a name to a Web site, BBS, or real person, and are too lazy to think of one yourself. Also, if the Web site/BBS/person you are giving the information to tries to crosscheck the city, state, zip, or area code, it will check out.

**Author:**  
Ian Turner



# Webbrowser „Mozilla“



The screenshot shows the Mozilla Help interface. At the top, there are navigation buttons (back, forward, search) and a search bar. Below that is a table of contents with categories like 'Glossary', 'Index', 'Search', and 'Contents'. The 'Contents' section is expanded, showing a list of topics including 'Help and Support Center', 'Using the Help Window', 'Browsing the Web', 'Using Mail', 'Creating Web Pages', 'Customizing Mozilla', and 'Using Privacy Features'. The 'Using Privacy Features' item is selected, leading to a page with the following text:

### Using Privacy Features

Your browser includes features you can use to help safeguard your privacy as you surf the Internet.

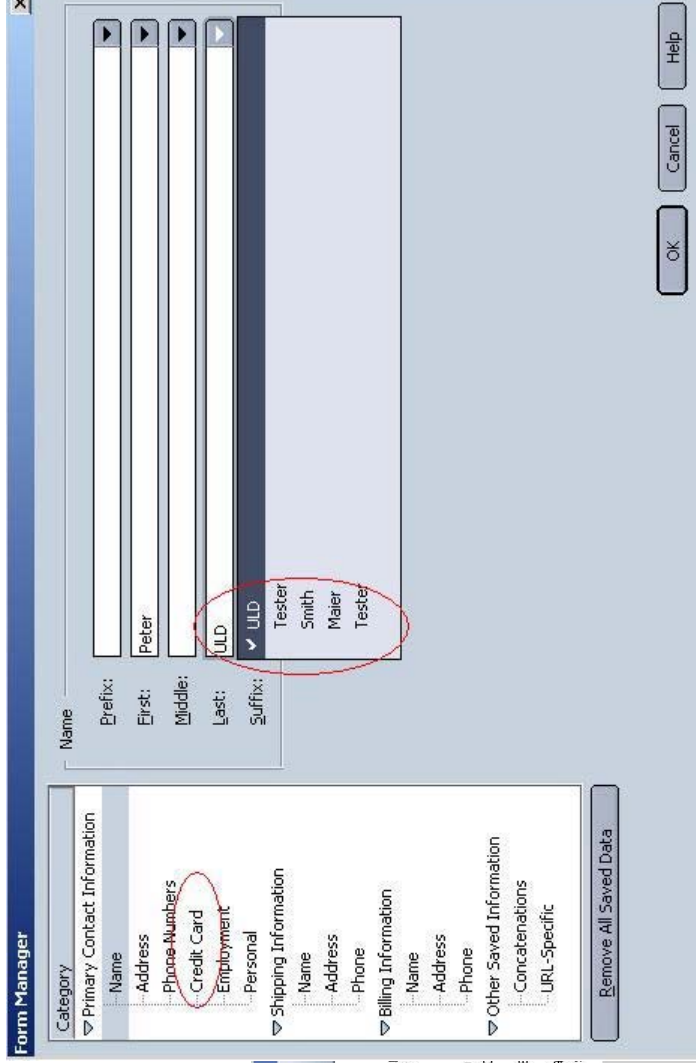
Some web sites publish their privacy policies. You can use the information on how to customize your browser to help protect your privacy.

For information about related Netscape products, see the Netscape website.

For general information about privacy and security, see the Mozilla website.

**Privacy Topics:**

- [Privacy on the Internet](#)
- [Using the Cookie Manager](#)
- [Using the Password Manager](#)
- [Using the Form Manager](#)
- [Encrypting Stored Sensitive Information](#)
- [Managing Images](#)
- [Privacy & Security Preferences](#)



The screenshot shows the Mozilla Form Manager dialog box. It has a title bar 'Form Manager' and a close button. The dialog is divided into two main sections. The top section is for 'Primary Contact Information' and contains the following fields:

- Name: [Empty]
- Prefix: [Empty]
- First: Peter
- Middle: [Empty]
- Last: [Empty]
- Suffix: ULD

The bottom section is for 'Other Saved Information' and contains the following fields:

- Name: [Empty]
- Address: [Empty]
- Phone: [Empty]
- Name: [Empty]
- Address: [Empty]
- Phone: [Empty]
- Concatenations: [Empty]
- URL-Specific: [Empty]

At the bottom right, there are buttons for 'OK', 'Cancel', and 'Help'. A red circle highlights the 'Suffix' field in the top section, which is currently set to 'ULD'. Below it, a dropdown menu is open, showing the following options: 'Teste...', 'Smith', 'Maier', and 'Teste...'. The first option 'Teste...' is selected and highlighted.

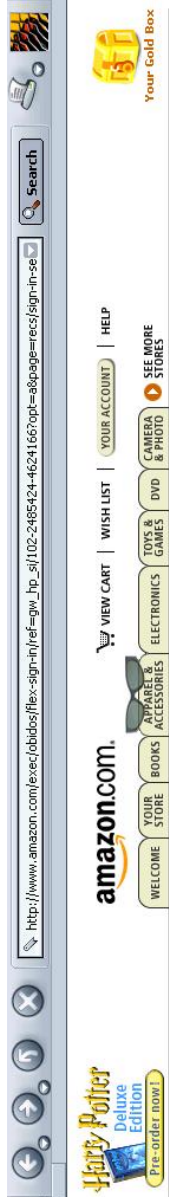
## Privacy on the Internet

This section summarizes some background information about privacy on the Internet. It also describes several things you can do to help safeguard your own privacy. It is not intended to provide a complete description of Internet privacy issues.

In this section:

- [What Information Does My Browser Give to a Web Site?](#)
- [What Are Cookies, and How Do They Work?](#)
- [How Can I Control Web Pages in Email Messages?](#)
- [How Can I Make Sure Unauthorized People Don't Use](#)





What is your e-mail address?

My e-mail address is

Do you have an Amazon.com password?

No, I am a new customer.

Yes, I have a password:

[Sign in using our secure server](#)

- [Forgot your password?](#) [Click here](#)

- Has your e-mail address changed since your last login?

The secure server will encrypt your information. If you receive a message when you tried to use our secure server, sign in using our standard server.

### New Customer Benefits

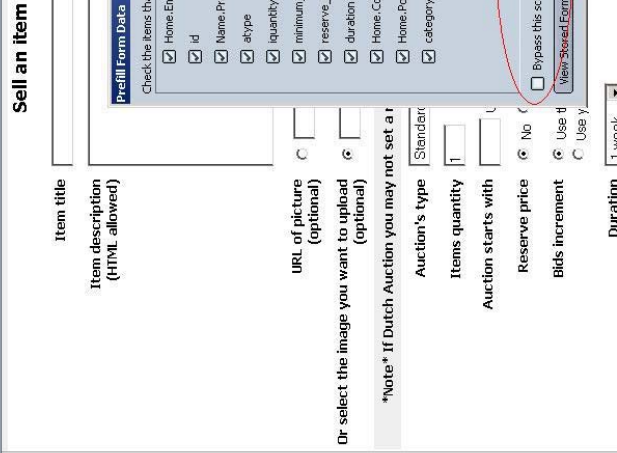
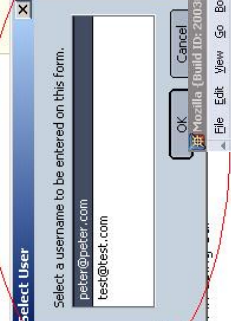
- Personalize Amazon.com: By telling us your interests, we'll remember them and personalize the site just for you.

### Free and easy!

Creating a new account requires NO credit card or personal information until you decide to buy.

### Watch an Animated Demo!

How customer? [Click to learn about searching, browsing, and shopping at Amazon.com.](#)



[Amazon.com Home](#) | [Dir](#)

[Our International Sites: Canada](#) | [United Kingdom](#)

[Help](#) | [Shopping Cart](#) | [Your Account](#)

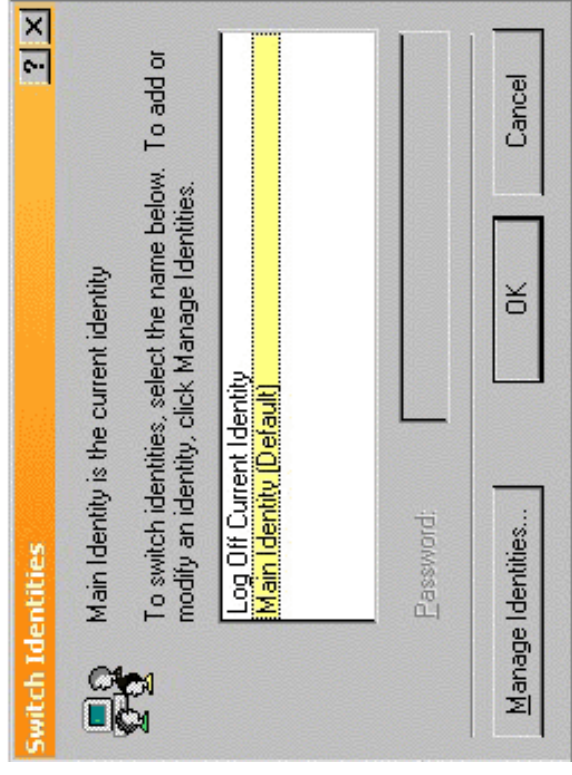
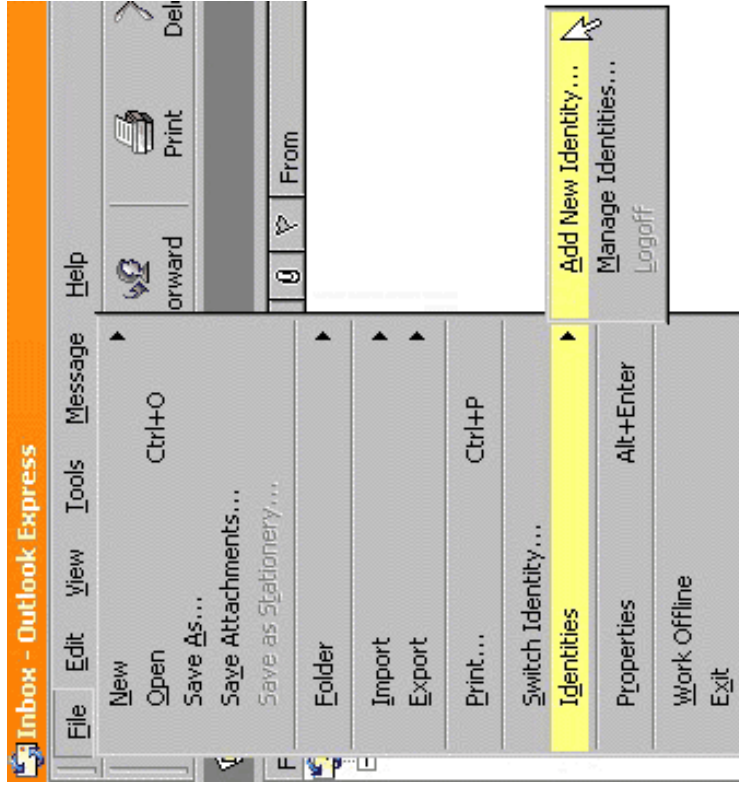
[Investor Relations](#) | [Press Release](#)

[Conditions of Use](#) | [Privacy Notice](#) © 1996-2000

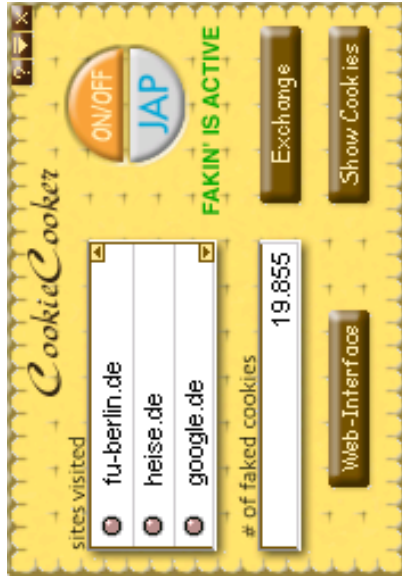
# Webbrowser „Mozilla“



# Mail-Software „Outlook Express“



*Identitätsmanagement und E-Health*



CookieCooker Web-Interface - Microsoft Internet Explorer

Adresse: http://cookie-cooker/identitylist?darst=2

Status: CC active / JAP inactive  
 CookieCooker Homepage  
 Main Page Web Interface

### Identities / Cookies / login data

only identities (login data) | alphabetically by the id's name | Overview

Web site	Identität	password protection	Data	Cookie	Comments
<input type="checkbox"/> 217.160.136.83	Henry	Yes	Login	16.06.2004	
<input type="checkbox"/> ebay.de	Henry	Yes	Login	end of session	
<input type="checkbox"/> ebay.de	Henry	Yes	Login	-	
<input type="checkbox"/> heise.de	imtest	No	Login	end of session	

Change setting of the marked identities to: delete id [Submit]

CookieCooker Web-Interface version 0.01.24

## „CookieCooker“

Select identity

on Site: **ebay.de**

Which identity/cookie do you want to use?

select automatically

- ebay.de
- Henry (15.36:15)
- Henry (17.06.2003)

create a new identity

select ID where still today not used

use AutoLogin

store decision

OK



# Single Sign-On- Dienst „Yodlee“

**YODLEE**

**Login** [Help ?](#)

**Already a Member?**  
**Sign in!**  
 My Yodlee ID:   
 Password:   
   
[Tell a Friend](#)

**All Your Accounts**  
 on one secure page.  
 My Yodlee gives you free, one-password access to all your **News** accounts.

↑ **IT'S FREE!**

My Yodlee is [private](#), [secure](#), and [insured](#).

**Wells Fargo**  
 Let remote transfer app **REGISTER**  
 Account Type (View details) 18255000  
 PIN MA (View details) 7475 0000  
 Statement (View details) 0827 0000  
 Card Balance

**Chubb Bank**  
 Let remote transfer app **REGISTER**  
 Account Type (View details) 888 0000  
 Card Balance (View details) 0000 0000  
 Statement (View details) 0800 0000  
 Total Balance

**American Express**  
 Let remote transfer app **REGISTER** (View details)  
 Low interest rate on app **REGISTER** (View details)  
 Available Credit



[Privacy Policy](#) | [Security Policy](#) | [Help](#) | [Yodlee Corporate Home](#)  
 Copyright © 2003 Yodlee, Inc. All rights reserved.



Add a New Account Preferences Refresh All

**Welcome intrest** July 2, 2003, 5:21 PM

You have no new alerts.

**Get started by adding accounts**

**Things to Try**

- See all my accounts
- Add an account
- Change my preferences
- Chart my net worth
- Share a statement with an advisor
- Install My Yodlee Assistant

**Shortcuts**

Go to Account Summary

**My Balances** edit - x

Stay informed about all your account balances -- including frequent flyer programs.

Citibank Online  
American Express Cards  
Provident  
United Airlines - Mileage Plus  
American Airlines  
AA-Advantage  
Plus many more...

➔ [Add a financial account](#)  
or [Add a frequent flyer account](#)

**My Messages** edit - x

Check all of your email in a single glance and go directly to your inbox without entering your username and password.

Hotmail  
Yahoo! Mail  
AOL Mail  
Excite Inbox  
Mail.com  
Plus many more...

➔ [Add an email account](#)

**My Reminders** edit - x

Don't miss a bill due date or an important appointment

Yahoo! Calendar  
FirstUSA  
MENA Credit Card  
eBay  
AT&T Wireless Services  
Plus many more...

➔ [Add a financial account](#)  
or [Add an online calendar](#)

**My Transactions** edit - x

See the most recent transactions for your bank, credit card, investment and other accounts.

MENA Credit Card  
FirstUSA  
Citibank Online  
Chase  
Discover Card  
Plus many more...

➔ [Add a financial account](#)

**My Bills** edit - x

Easily view and manage your bills with My Yodlee.

FirstUSA  
CapitalOne  
American Express Cards  
AT&T Wireless Services  
MCIWorldCom  
Plus many more...

➔ [Add a credit card account](#)  
or [Add a utility bill account](#)

Already pay your bills online? [Add your bill pay account.](#)

**My Investments** edit - x

No matter where you invest, you can consolidate all of your holdings here.

Yahoo! Calendar  
Fidelity Investments  
Ameritrade (formerly Datrek Online)  
E\*TRADE  
Charles Schwab  
Ameritrade  
eBay  
MENA Credit Card  
AT&T Wireless Services  
Plus many more...

➔ [Add an investment account](#)

**My News** edit - x

Stay on top of the latest news. Some of the more popular sources are listed below, but you can choose from many others, too!

USA TODAY  
 Bloomberg.com  
 CNET News.com  
 CNN/nr  
 ESPN.com  
 ZDNet Tech Briefs

➔ [Add the selected accounts](#)  
or [Add another news account](#)

**Auto-Login** - x

When you add online accounts to My Yodlee, you can link directly to those web sites -- without having to re-enter your user ID or passwords.

# Single Sign-On- Dienst „Yodlee“



Microsoft .NET Passport

**One name. One password.**

**One easy way to Sign in online.**

- ▶ Look for the .NET Passport **Sign In** button!
- ▶ Use **one name and password** to sign in to all .NET Passport-participating sites and services.
- ▶ Store personal information in your .NET Passport profile and, if you choose, automatically share that information when you sign in so that participating sites can provide you with personalized services.

And .NET Passport is free!

**Security**

Sign in on any computer that has Internet access... .NET Passport uses powerful online security technology and follows a comprehensive privacy policy to help protect your profile information. You manage your information-sharing options.



Register for your free .NET Passport today!

# Single Sign-On- Dienst „Passport“

Register for your **FREE** .NET Passport today!

**Members**

- ▶ [Get help](#)
- ▶ [View or edit your profile](#)
- ▶ [Reset your password](#)
- ▶ [View participating sites](#)
- ▶ [Notice: Express purchase has been discontinued](#)

**Businesses**

- ▶ [About .NET Passport](#)
- ▶ [Developer information](#)
- ▶ [Getting started](#)

**International**

 .NET Passport around the world

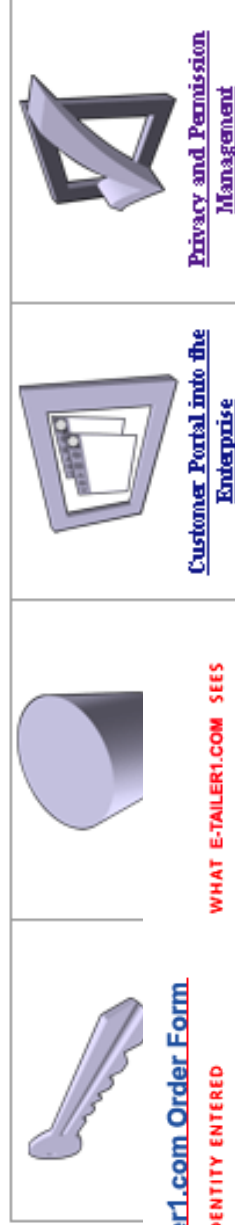
# Identitätsmanagement: serverseitig „Managing your identity on your behalf“

**Persona**  
e-Identity Solutions

Enterprise e-Identity Single Sign-In Platform **eBay**



The benefits of Persona Enterprise e-Identity include:



## E-tailer1.com Order Form

### TRUE IDENTITY ENTERED

Name: John Smith  
Address: 1 Main Street  
Address: 5th Floor  
City: Kansas City  
State: KS  
Zip: 66102  
email: smith@isp.com

### WHAT E-TAILER1.COM SEES

Name: iPrivacy101  
Address: &936jxW8725  
Address: \*%6R  
City: Kansas City  
State: KS  
Zip: 66102  
email: 101@iprivacy.com

**iPrivacy technology encodes this information** >>

### TRUE IDENTITY ENTERED

Name: John Smith  
Address: 1 Main Street  
Address: 5th Floor  
City: Kansas City  
State: KS  
Zip: 66102  
email: smith@isp.com

### WHAT E-TAILER1.COM SEES

Name: iPrivacy101  
Address: &936jxW8725  
Address: \*%6R  
City: Kansas City  
State: KS  
Zip: 66102  
email: 101@iprivacy.com



**LIBERTY ALLIANCE**  
project



UNABHÄNGIGES LANDESZENTRUM  
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

# Identitäts-Provider und -Broker: e-Notare

**PRIVADOR**

## Defenders of the e

### About Identity Manager

An identity is something that represents you in the digital world. You can have multiple identities, eg. one that represents you at the bank and the other that represents you at your phone service provider. You can use one identity to sign business documents and another to sign personal documents. See "Under the hood" for more information.

**Privador TrueSign Identity Manager**

Identity	Certificate	Notary
Mac	M. McTopp	GNS
MCTopp	M. McTopp	GNS
Marit Köhntopp privat	M. McTopp	Privacy-Notar



# „ID-Manager Freiburg“

**SPP Sicherheit – PDA7.3**


Ansicht Einstellungen Info

Verfügbare Anwendungen

	Adressen		Aufgaben		Browser
	E-Ticket		Geldbörse		Kalender
	Notepad		Notizen		Rechner

Start Anonym-ID 10:50

**ID-Manager: Identität wechseln**

 Die Anwendung "Geldbörse" hat folgende persönliche Daten vom ID-Manager angefordert:

Vorname:	Wilhelm
Nachname:	Weber
Strasse:	Kennedyallee 40
PLZ:	53170
Ort:	Bonn
Kontonu...:	123 456 7
BLZ:	100 000 00
Bank:	Geldinstitut Bonn

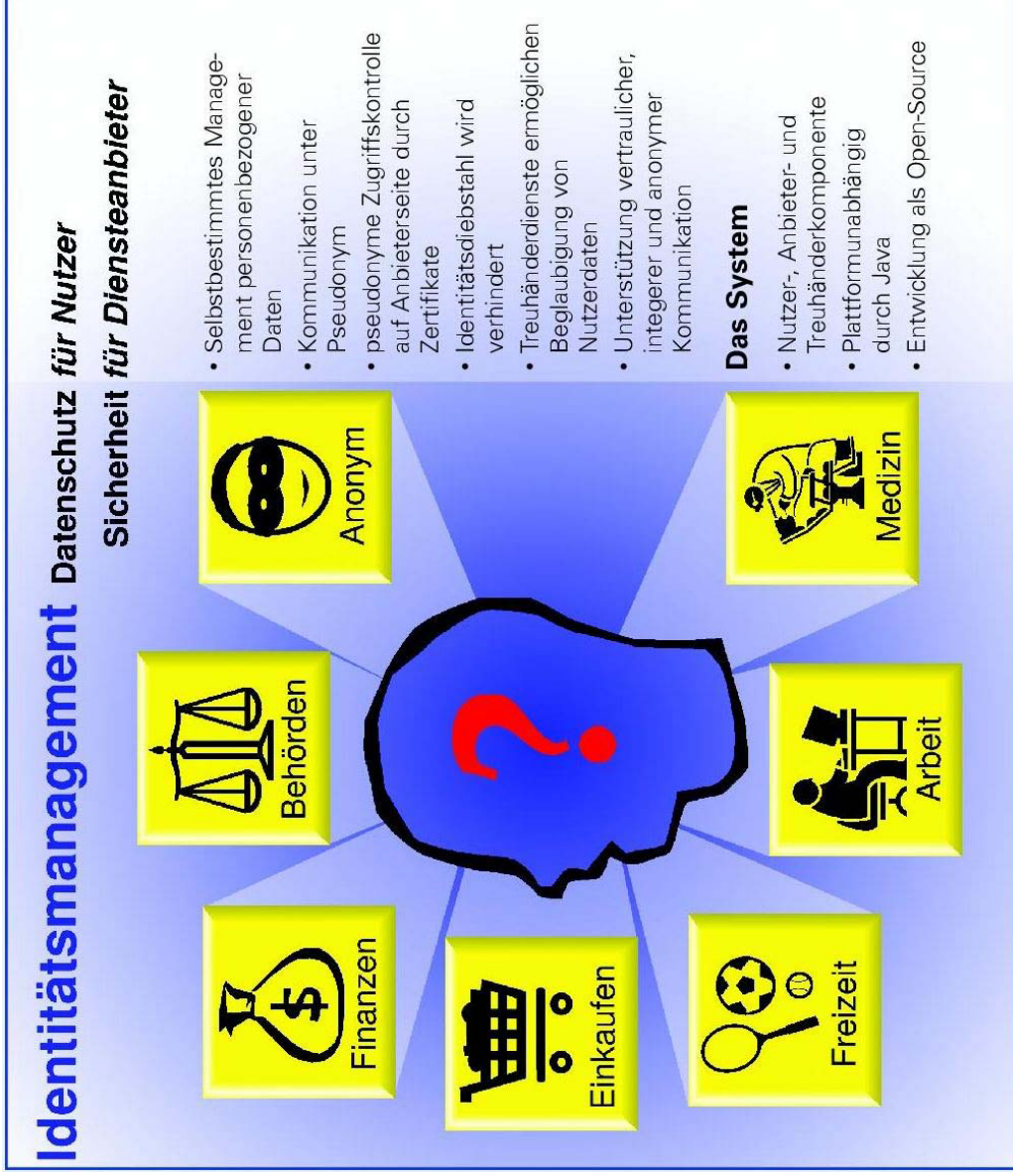
Die rot markierten Daten werden jedoch von der aktuellen Identität geschützt.

Weiter...

Start Anonym-ID 11:07



# „DRIM - Dresden Identity Management“



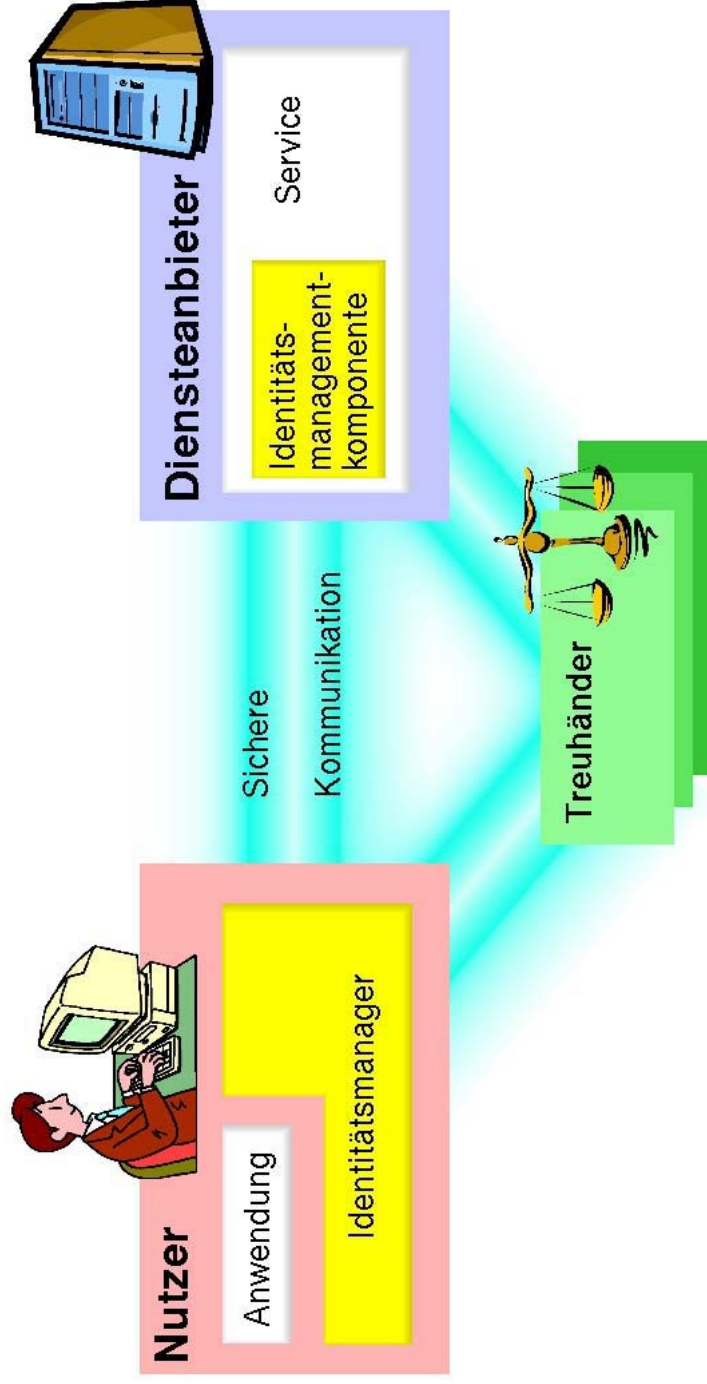
# Überblick



- **Identitätsmanagement:**  
Nutzergesteuerter Datenschutz
- **Beispiele aus Praxis und Forschung:**  
Password Manager, Single Sign-On, Form Filler ...
- **Konzepte für nutzergesteuertes Identitätsmanagement:**  
Mit Pseudonymen, Credentials, History-Funktion, 3<sup>rd</sup> Parties
- **Identitätsmanagement im Bereich E-Health:**  
Rollen, Verfahren, Szenarien
- **Fazit und Ausblick**



# Identitätsmanagement nicht nur beim Nutzer



## Kriterien - Werden sie erfüllt?

- Steuerung durch den Nutzer
  - **Nachvollziehen** der Kontrolle durch den ID-Manager
  - komfortable **Speicherung** serverseitig
  - **Datei** häufig **Speicherung** durch Nutzer
  - für A **zu wenig** **Steuerung** durch Nutzer
- **Verbindlichkeit**
  - nicht allein in **Speicherung** Systems möglich
  - Zure **Speicherung** digitale Signaturen)
  - Binde **Speicherung** an Personen (**Credentials**)
- **Interoperabilität**
  - offene **Star** **kaum** **berücksichtigt** **Ausbaufähigkeit**
- **Datensicherheit**
  - sowohl in **keine** **Realisierung**
  - ... als **Realisierung**
  - insbesondere: **zugrundeliegende Anonymität**



# Überblick



- **Identitätsmanagement:**  
Nutzergesteuerter Datenschutz
- **Beispiele aus Praxis und Forschung:**  
Password Manager, Single Sign-On, Form Filler ...
- **Konzepte für nutzergesteuertes Identitätsmanagement:**  
Mit Pseudonymen, Credentials, History-Funktion, 3<sup>rd</sup> Parties
- **Identitätsmanagement im Bereich E-Health:**  
Rollen, Verfahren, Szenarien
- **Fazit und Ausblick**





## Nutzergesteuertes Identitätsmanagement in Deutschland: Fundierung im Recht

- **Einhaltung des Datensparsamkeitsgrundsatzes (§ 3a BDSG):**

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der **Anonymisierung und Pseudonymisierung** Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

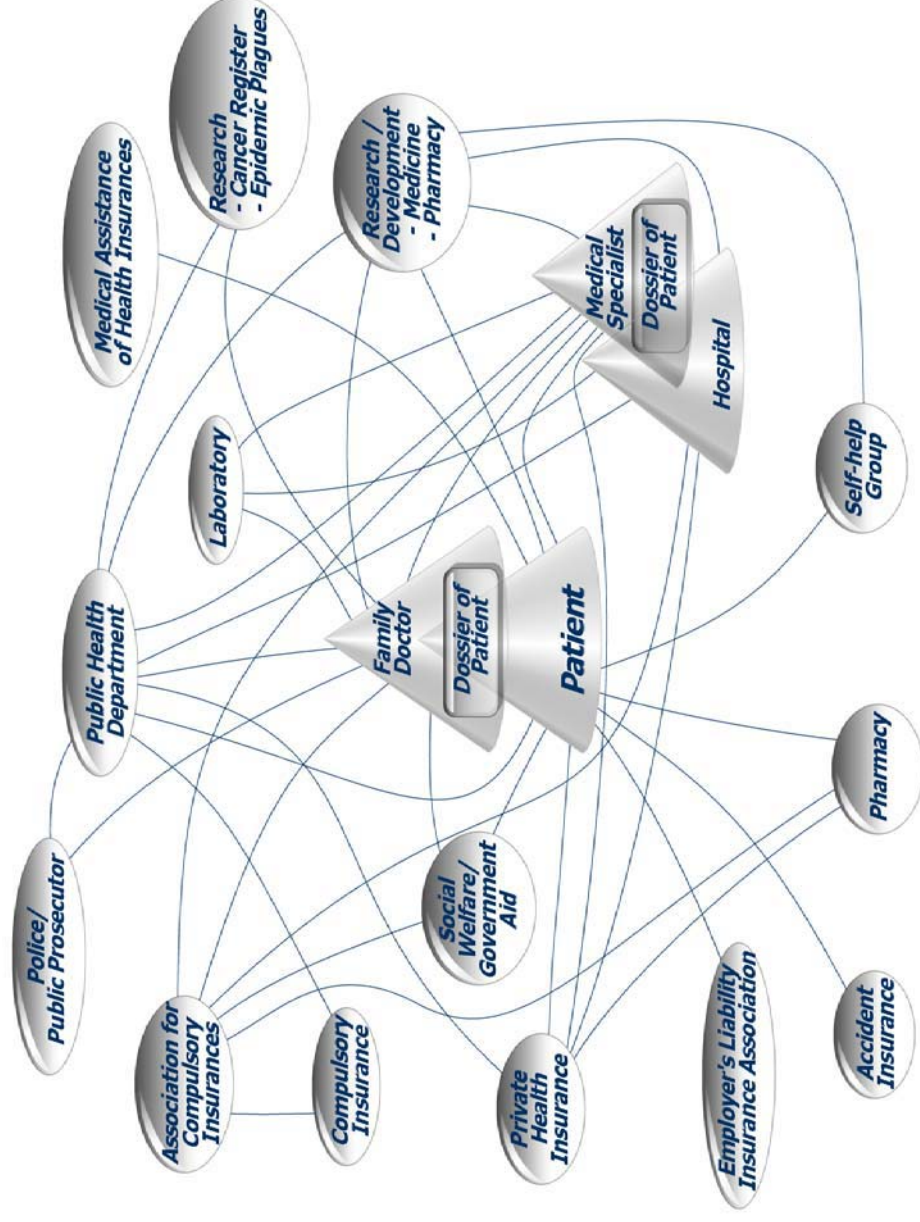
- **Einhaltung des § 4 Abs. 6 Teledienstschutzgesetz:**

Der Diensteanbieter hat dem Nutzer der Inanspruchnahme von Telediensten und ihre Bezahlung **anonym oder unter Pseudonym** zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.





# Verschiedene Rollen im Bereich E-Health



## **E-Health: Verfahren 1/2**

- **Patient - Arzt (in Praxis, Krankenhaus oder Labor):**
  - Medizinische Beratung (telefonisch oder online)
  - Erreichbarkeitsmanagement
  - Abruf von Labor-Ergebnissen
  - Notfallversorgung
- **Patient - Krankenversicherung / Arzt - Krankenversicherung**
  - Abrechnung
  - Bonus-Programme
- **Arzt - Arzt:**
  - Bilateraler Informationsaustausch
  - Gruppenweiterbildung





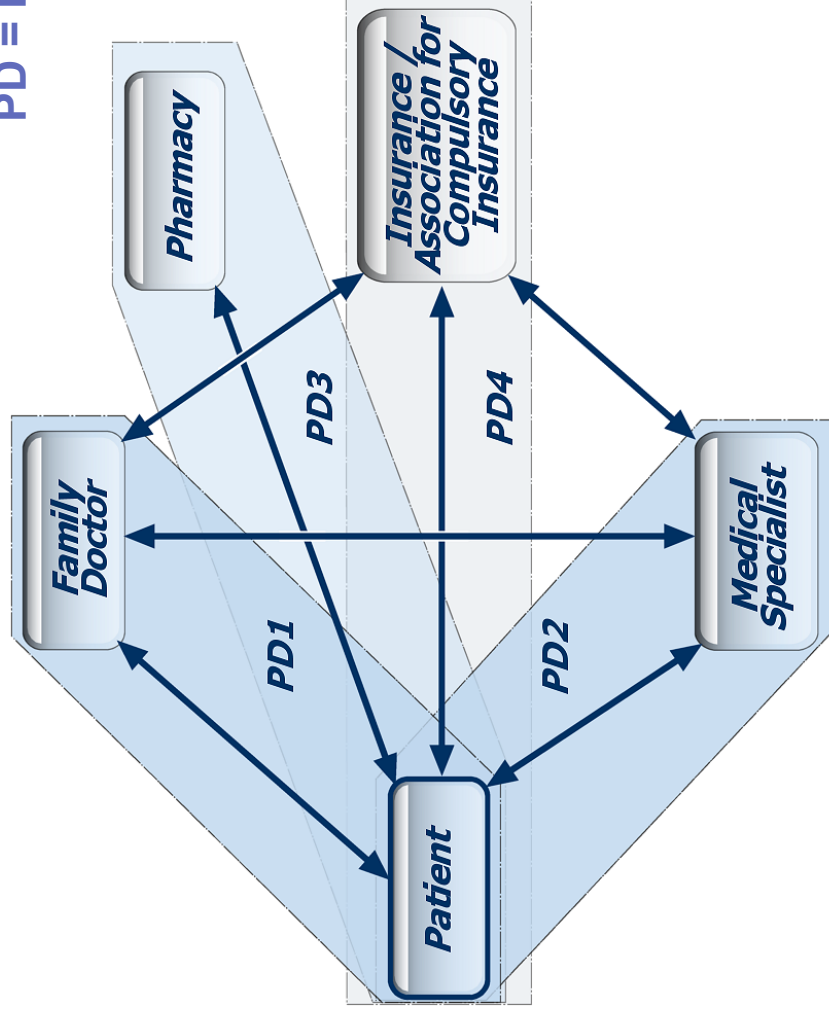
## E-Health: Verfahren 2/2

- **Patient - Apotheke**
  - **Beratung**
  - **Einkauf (mit oder ohne Rezept, online oder offline)**
- **Patient - Forscher:**
  - **(Langzeit-)Forschung mit (anonymen/pseudonymen) Daten**
- **Patient - Staat:**
  - **Einfluss auf gesünderen Lebensstil**
  - **Statistikerstellung als Planungsgrundlage**

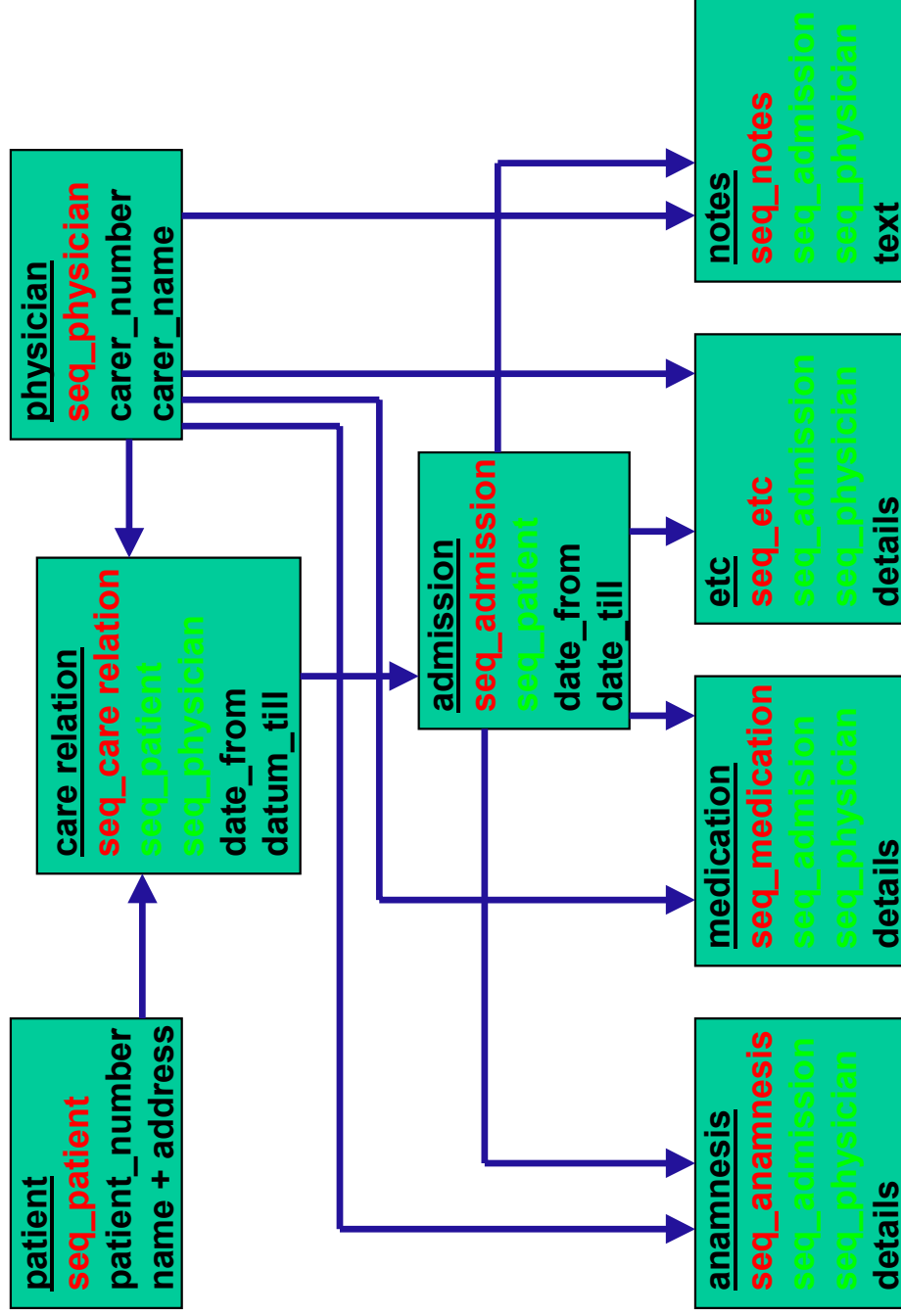


# Pseudonym Domains eines Patienten (Ausschnitt)

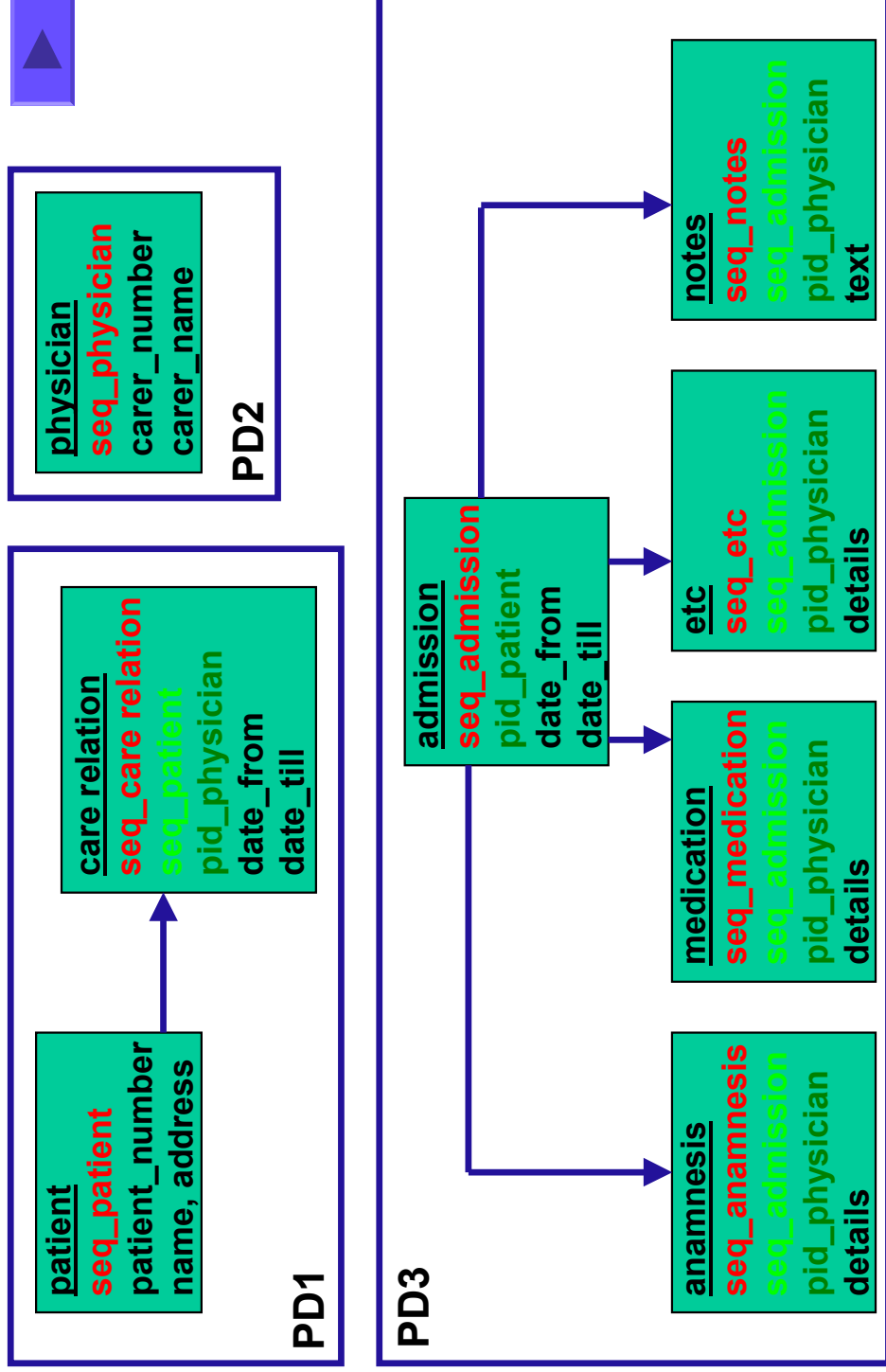
PD = Pseudonym Domain



# Hospital Information System: Basic Tables and Relations



# Privacy-Enhancing Hospital Information System: Some Pseudonym Domains



---

# Die Praxis: Beispiele für Online-Beratung im Internet



UNABHÄNGIGES LANDESZENTRUM  
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

---

*Identitätsmanagement und E-Health*

# Online-Beratung mit Pseudonym + Passwort

The screenshot shows a Netscape browser window with two tabs. The active tab is titled "Drogenberatung - Jugendhilfe - Netscape" and displays a website for "Drogenberatung". The website has a navigation menu with icons for "Drogenberatung", "Kokain", "synthetische Drogen", and "chat". Below the menu, there are logos for "ji" (Jugendberatung und Jugendhilfe e.V.) and "hessen Sozialnetz". A search bar is visible at the top right of the page content.

The second tab is titled "Email - Netscape" and displays a page titled "Anonyme e-mail-Beratung". The page content includes the following text:

Die "Anonyme e-mail-Beratung" ermöglicht es Ihnen, anonym Fragen an uns zu stellen und Antworten von uns zu erhalten.

Um das Angebot zu nutzen brauchen Sie ein Login und ein Passwort. Unter diesem Login können Sie mehrere e-mails mit Ihren Fragen an uns senden und Sie erhalten darauf von uns entsprechende Antworten.

Falls Sie noch kein Login besitzen, können Sie sich [hier anonym anmelden](#).

Below the text is a login form with two input fields labeled "Login:" and "Passwort:", and a button labeled "Einloggen".

# Online-Beratung mit Pseudonym und E-Mail-Adresse

**Netscape** Beratung - Netscape

beratungsnetz.de/ anmelden/index.php

> Anmeldung

ldung  
e sich Ihren Benutzernamen registrieren lassen.

meldung

Benutzername:  Fortsetzen

E-Mail-Adresse:

bekommen Sie eine  
on uns geschickt.

eser E-Mail enthalten !

**35**  
zone35  
multimedia  
agentur

**Datenschutzerklärung**

Bei jedem Zugriff eines Nutzers auf eine Seite aus dem Angebot von das-beratungsnetz.de werden Daten über diesen Vorgang in einer Protokolldatei (Webserver-Logfile) gespeichert. Im einzelnen wird über jeden Abruf folgender Datensatz gespeichert:

Name der abgerufenen Datei, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Meldung, ob der Abruf erfolgreich war, Typ des verwendeten Webbrowsers, IP-Adresse, die dem Nutzer von seinem Internet-Zugangsprouder für die Nutzung von Internetdiensten zugewiesen wurde. Die gespeicherten Daten werden nur zu statistischen Zwecken vom Betreiber zone35 - new media anonymisiert ausgewertet. Eine Weitergabe personenbezogener Daten an Dritte findet nicht statt.

Aus technischen Gründen werden die Inhalte des Chats mit Nickname, Datum und der Uhrzeit in einer temporären Protokolldatei gespeichert. Diese Protokolldatei ist für die Anzeige im Chat erforderlich. Die Einträge in dieser Protokolldatei werden vom Chatssystem nach Verfall der Informationen automatisch gelöscht.

Der Betreiber zone35 new media, ist nicht für die Sorgfalt der abgeschlossenen Beratungsverbindungen im Umgang mit sensiblen Daten von Nutzern verantwortlich. Insbesondere nicht für etwaige Notizen und oder Mitschriften, die sich ein Berater während einer Sitzung in irgendeiner Form eigenmächtig anfertigt.

UNABHÄNGIGES LANDESZENTRUM  
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

# Online-Beratung mit SSL-verschlüsselten Formularen

**Verschwiegenheitspflicht & Datensicherheit - Netscape**

Datei Bearbeiten Ansicht Gehe Communicator Hilfe

Leesezeichen Adressleiste Adresse: <http://www.psychologische-fem-beratung.de/~verschwiegenheit.html>

**Anonyme Beratung**

- Legen Sie Wert auf **Anonymität uns gegenüber**, so können Sie auf die Angabe von Name und Anschrift verzichten und teilen uns nur eine E-Mail-Adresse mit, aus der Ihr Name nicht ersichtlich ist. In diesem Fall ist eine Vorauszahlung der Beratungsgebühr notwendig.
- Vollständige Sicherheit und Anonymität von Datenübertragungen im Internet sind prinzipiell nicht gewährleistet.
- Daher sollten Sie auf jeden Fall unsere **SSL-verschlüsselten Formulare** (Secure Socket Layer) nutzen, die es Dritten erschweren, übermittelte Inhalte mitzulesen.
- Falls diese mit Ihrem Browser nicht funktionieren sollten, bieten wir die Möglichkeit, ein Beratungsformular unter einem **Pseudonym** abzuschicken und die personenbezogenen Daten (Name und Anschrift) auf einem gesonderten Weg (Post, Fax oder E-Mail) unter Angabe des Pseudonyms nachzusenden.
- Alternativ gibt es auch ein **Textformular**, das inklusive Name und Anschrift mit jeder beliebigen Textverarbeitungsprogramm ausgefüllt und per Post, Fax oder PGP-verschlüsselter E-Mail an uns gesandt werden kann.
- Falls andere Personen Zugang zu dem von Ihnen benutzten Computer haben, sollten Sie unbedingt nach einer Internetsitzung, in der Sie ein Formular mit vertraulichen Informationen ausgefüllt haben, **das Browser-Programm ganz beenden**. Eventuell empfiehlt es sich vor dem Löschen der sog. History- und Cache-Einträge des Browser zu löschen.

**Datensicherheit im Internet**

**SSL: Secure Socket Layer**

**PGP-verschlüsselte E-Mail**

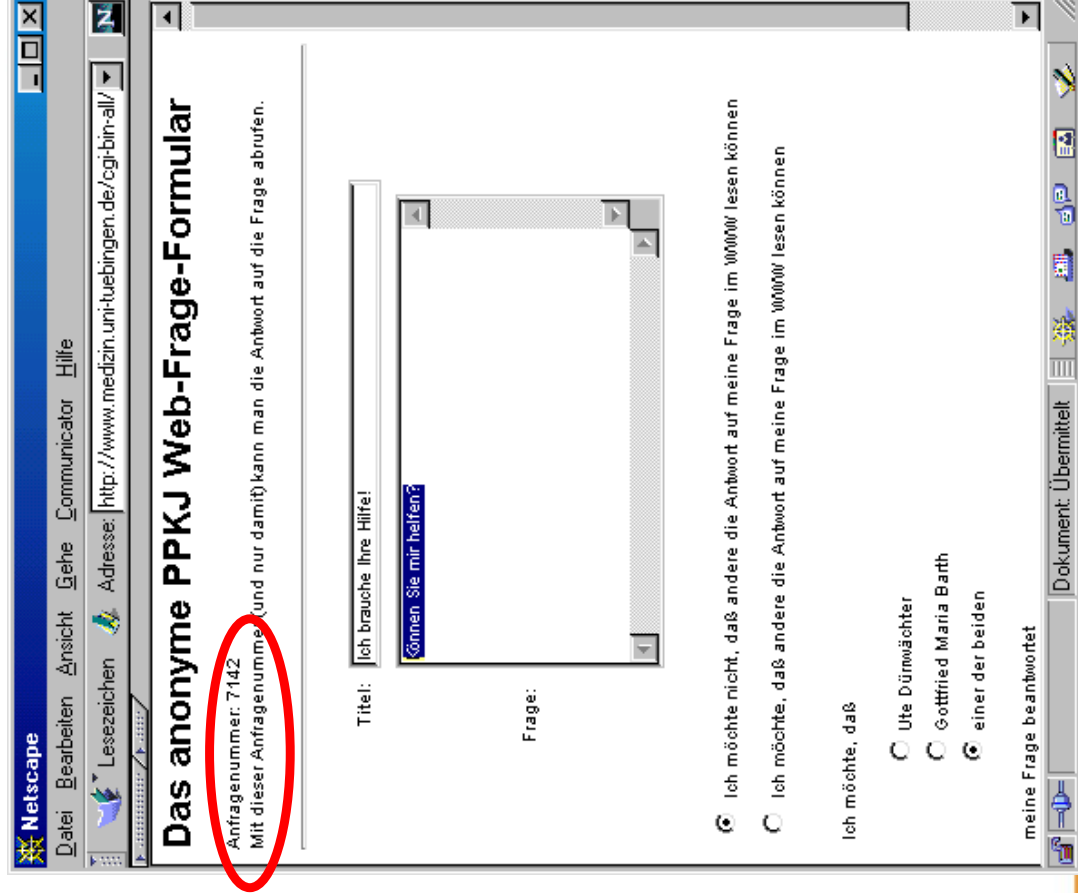
PGP (Pretty Good Privacy) gilt zur Zeit als Standardverschlüsselungsmethode für den E-Mail-Verkehr. PGP bietet den

Dokument: Übermittelt



# Online-Beratung per pseudonym abrufbarer Webseite

Pseudonym:  
Anfragenummer



## Fazit & Ausblick

- **Identitätsmanagement**
  - Wichtig für **Datenschutz in Nutzerhand**
  - Bisherige Ansätze unzureichend: **Zukunftskonzept**
  - Entwicklung **möglich und** - mit Aufbau von Signatur-PKI - **nötig**
- **Identitätsmanagement und E-Health**
  - Grundsätzlich **möglich**
  - Meist **weniger sinnvoll im Verhältnis Patient - Hausarzt:**
    - Ganzheitliche Sicht des Patienten bedingt Verkettabarkeit
    - Vertrauensverhältnis ist Voraussetzung
  - Bei **Neugestaltung** der Systeme zu durchdenken

- **Ausblick**

Mögliche **Applikation** im Projekt PRIME:  
bei Hospital San Raffaele del Monte Tabor (Italien)



## EU-Projekte: FIDIS und PRIME

- Network of Excellence „FIDIS - The Future of Identity in the Information Society“
- Integrated Project PRIME:



Information Society  
Technologies



# PRIME

Privacy and Identity Management for Europe

PROPOSAL NUMBER  
**A097-507591**

#### Vision:

Users can act securely and safely in the Information Society while keeping sovereignty of their private sphere.

#### Objectives:

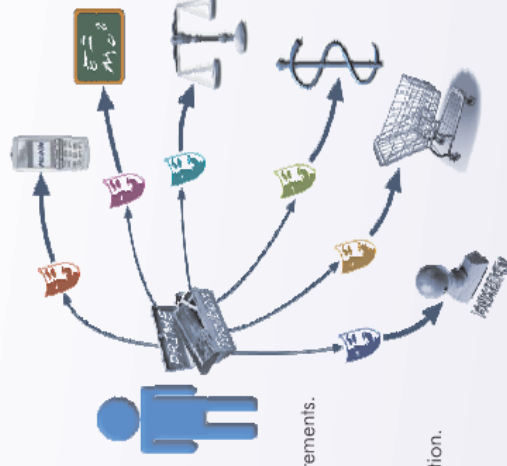
- Develop *solutions to empower individuals* to control their private sphere and manage their identities.
- Trigger pervasive deployment of *privacy-enhancing identity management* solutions.

#### Results:

- Legal, socio-economic, usability, and application requirements.
- Public integration framework.
- Public architecture & specifications.
- Application-driven prototypes.

**Exploitation:** Providing novel solutions for practical use and standardisation.

**Duration:** 4 years.



**Possible Application:**  
**Continuous care at home and on the move**

- Functions:**
- **Remote therapy management**
  - **Remote diagnosis**
  - **Emergency management**

**Andriy Pazyuk**

President of Privacy Ukraine, Kiev, Ukraine

## **Information Policy of Ukraine: Access, Transparency, E-governance**

### Introduction

Information policy observers in Ukraine could note constant struggle between transparency and secrecy tendencies. It has direct impact on the “public authority - civil society” relations influencing both sides of freedom of information: right to obtain and right to disseminate information freely. Both of them are indicators of democracy. The right to obtain information (right to access) is connected to the transparency of public management, good governance and citizens' participation in public affairs, the right to disseminate information freely - to press freedom and political pluralism. The competition of mentioned tendencies becomes apparent at political, regulatory and practical levels. Ukrainian politicians declare adherence to the transparency policy but the monitoring of legal changes shows non-correspondence of words and deeds.

### State Owned versus Public Domain

The Constitution of Ukraine adopted in 1996 contains a “right to freely collect, store, use and disseminate information by oral, written or other means of his or her choice” (Article 34). But it does not include a specific general right of access to information held by public authority [1]. Such gap is the source for the manipulations at the level of laws and under-laws regulations.

The 1992 Law on Information allows citizens to request access to official documents[2]. But the exceptions from the right to access are broad and vague. The Article 28 classifies information in terms of access mode as open information and information with restricted access. The Article 30 provides for the two types of restricted access information: confidential and secret. Confidential information shall be understood as data being possessed, used or disposed by certain natural persons, legal entities, to be disclosed at their discre-

tion, subject to conditions established by these persons. Secret information shall be understood as information, which contains data qualified by law as the state and other secrets, the disclosure of which will damage the person, society, and the state.

The mentioned Article 30 also provides that "the procedure for secret information circulation and protection shall be determined by relevant state bodies provided they abide by the requirements set forth in this Law; and "a relevant law shall determine the procedures and terms for disclosing secret information".

The requirements for the processing of state secret have been determined by the Law on State Secret [3]. But the processing of other secret information has not been regulated by laws yet. The Cabinet of Ministers exceeding its authority adopted the Regulation on the Rules of Accounting, Keeping and Usage of Documents, Editions and Other Material Carriers Containing Confidential Information Owned by State in 1998 [4]. The Regulation is in conflict with the Article 30 of the Law on Information according to which confidential information shall be understood as data being possessed, used or disposed by certain natural persons, legal entities but not state.

As the Law on Information does not provide for the interpretation of terms "open access information" and "other secrets, the disclosure of which will damage the person, society, and the state" such loopholes granted broad discretion of public authority when classifying information. The proprietary concept is used for the limitation of citizens' access to government-held information. A study by the Kharkiv Group for Human Rights Protection found sufficient overclassification of documents in 2000-2001 [5].

The concept of state property on information held by government presumes that it's discretion of public bodies' officials to decide what information could be of open access. Mainly it is limited to the information about official activity distributed by public bodies as a part of public relations campaigns. Such PR activity of public bodies is required by the Ukase of President on Additional Measures to Ensure the Publicity of the Governmental Bodies Activities of August 1, 2002 (N 683/2002). It ordered the Cabinet of Ministers to study the implementation of the Law on Information for the years 2000-2002.

The report on the implementation of the Ukase submitted by December 10, 2002 by the central and local executive bodies to the State Committee on Information contains among other statistical data of the access granted to open information [6]. According to the report "there were no refusals to provide open information". But it does not contain information on the rejected inquires with regard to the classified information which could be of public interest.

The attempt to legalize the proprietary concept with regard to the government-held information has been made by the law-enforcement agencies by submitting draft law to the Parliament (N 2663 of January 17, 2003). It provides among other for the amendments to the Article 30 of the Law on Information granting to the Cabinet of Ministers authority to adopt "regulation on the accounting, keeping and usage of documents and other carriers containing confidential information owned by state". It also aimed to amend the Law on Printed Mass-Media (Press) in Ukraine restricting the right to freely search, receive, fix, save, use and disseminate information to the information with open access.

The draft has been approved by the Parliament in a very little time by June 9, 2003. By this time Leonid Kuchma, the President of Ukraine, has not signed the draft law yet. The domestic and foreign experts found it very restrictive and violating freedom of information.

Such unexpected decision of the Parliament is in conflict with the previously adopted law On the Amendments to the Several Legal Acts on the Safeguards and Unhampered Fulfilment of the Human Right to Freedom of Speech (No 676-IV) signed by the President of Ukraine on April 3, 2003 as a result of the Parliamentary hearings devoted to freedom of speech in Ukraine held on December 4, 2002. The Law No 676-IV introduces administrative liability for the violation of the right to information (failure by public authority to provide information to the public upon request, for releasing incomplete information and/or for undue delay in the release of information) amending the Code of Administrative Offences with the new Article 212-3. Amendments to the Article 17 of the Law on State Support of Mass-Media and Social Safeguards to Journalists release journalists from the liability for the unintentional dissemination of false information. It amends the Law on Information prohibiting censorship (Article 45-1) and also amends the Article 30 of the Law on

Information with the provisions allowing dissemination of classified information without permission of its owner if: 1) such information is of public interest; and 2) the right of public to know prevails the owner's right for the protection.

The provisions of the Law N 676-IV may be considered as the first attempt to introduce concept of public domain information into Ukrainian legal framework. Further elaboration of the comprehensive government information policy framework for the management and open dissemination of government-held information is required.

Perspectives of ICT usage for the improvement of access and transparency

The dissemination of information about government activity, virtual interfaces between citizens, national and local authorities as well as provision of public services on-line are the few examples of the E-gov services usage as effective tools to facilitate an environment of transparency and better governance.

It is already proved that wide dissemination of government-held information using public networks improves efficiency and effectiveness of governance and has multiplier effect for the development of social capital and for economic welfare.

The Ukase of President of July 2000 "On the Measures for the Development of National Inclusive Internet Information Network and for the Provision of a Broad Access to this Network in Ukraine" obliges public bodies to "establishment until the end of 2000 of the order of distributing the information on the public bodies activity and the completion of creation of the official web-sites by the central bodies of executive power" [7].

The Cabinet of Ministers approved the Order on the Dissemination in the Internet Information on the Activity of the Bodies of Executive Power in January 2002 (N 3) [8]. The Order provides for two ways of information dissemination: via public bodies official web-sites and by the creation of the United Web-Portal of the Cabinet of Ministers of Ukraine integrating public bodies official web-sites information. The Order determines the competence of public bodies, procedure of on-line publication as well as the list of the mandatory information to be provided.

The study of Internews-Ukraine found the positive influence of the Order N 3 resulting in more factual content and regular updates of the information in 2002 [9].

The Order of the Information Fulfilment and Technical Safeguards of the United Web-Portal of the Public Bodies of Executive Power and Order of Public Bodies Web-Sites Functioning has been jointly enacted by the State Committee on Information Policy, TV and Broadcasting, and the State Committee on Telecommunications in November 2002 [10]. It reduces the mandatory list of information for its distribution via United Web-Portal to official news, announcements of meetings, visits and their results, press-releases, official statements, interviews, speeches - to be disseminated, if not immediately, in 1-3 days; and statistical & analytical information - to be disseminated when appropriate.

It is expected sufficient improvement of E-gov services based on identification and digital signatures usage by 2005. Such schedule is fixed in the Cabinet of Ministers Enactment on the Measures for the Creation of Electronic Information System 'Electronic Government' adopted in February 2003 [11]. The plans of the Government based on the legal framework created by the Laws on Electronic Digital Signature [12] and the Law on Electronic Documents and Electronic Documents Circulation adopted in May 2003 and entering in force from January 1, 2004 [13].

The mentioned regulations create, in general terms, the new interactive form of interrelations between civil society and government. It is to improve effectiveness of public management surely. But its effect could be multiplied in social and economical dimensions if the state policy with regard to the dissemination of information held by government would be improved.

To confirm the barely written the statistical data of the public sector information (PSI) value comparative study could be used. It is found sufficient discrepancy in Europe and US of the PSI economic value. The amount, EU governments spend in creating information, is around 9.5 bn Euro each year, and the central estimate of economic value of this data is 68 bn Euro. In the USA the investment value is double than in the EU, but the economic value - at 750 bn Euro. The



report imputes it partly to US public sector information policy based on strong freedom of information law, no government copyright, fees limited to recouping the cost of dissemination, and no restriction on reuse [14].

The survey recently published by UNESCO contains recommendations for the development of government information policy framework based on the concept of public domain information wide dissemination [15]. It could be used for the improvement of access and transparency in Ukraine.

- 1 Constitution of Ukraine, 1996.
- 2 The Law on Information of October 2, 1992 (N 2657-XII) as amended by the Laws of April 6, 2000 (N 1642-III), of February 7, 2002 (N 3047-III), of April 3, 2003 (N 676-IV).
- 3 The Law on State Secret of January 21, 1994 (N 3855-XII) in the redaction of Law of September 21, 1999 (N 1079-XIV) as amended by the Law on June 19, 2003 (N 971-IV)
- 4 Cabinet of Ministers Regulation on the Rules of Accounting, Keeping and Usage of Documents, Editions and Other Material Carriers Containing Confidential Information Owned by State of November 27, 1998 (N1893) as amended by the Enactments of November 29, 2001 (N 1601), of March 13, 2002 (N 281).
- 5 Kharkiv Group for Human Rights Protection, Analysis of Practice Access to Governmental Information;  
<http://www.khpg.org/index.php?au=0322001000>
- 6 <http://www.article19.org.ua/publications/report.html>
- 7 The Ukase of July 31, 2000 (N 928/2000)
- 8 Enactment of January 4, 2002 (N 3) as amended by the Enactment of June 16, 2003 (N 905).

- 9 See: An Analysis of Internet Access to Information of the Institutions of the State of Ukraine;  
[http://gipi.internews.ua/ukr/activity/analyst/Ukraine\\_Internet\\_Analysis\\_Edit.doc](http://gipi.internews.ua/ukr/activity/analyst/Ukraine_Internet_Analysis_Edit.doc)
- 10 Enactment of November 25, 2002 (N327/225).
- 11 Enactment of February 24, 2003 (N 208).
- 12 The Law of May 22, 2003 (N 852-IV).
- 13 The Law of May 22, 2003 (N 851-IV).
- 14 PIRA International (2000), "Commercial Exploitation of Europe's Public Sector Information", Final Report to the European Commission, Directorate General for the Information Society;  
[ftp://ftp.cordis.lu/pub/econtent/docs/commercial\\_final\\_report.pdf](ftp://ftp.cordis.lu/pub/econtent/docs/commercial_final_report.pdf)
- 15 Draft Policy Guidelines for the Development and Promotion of Public Domain Information / prepared by Paul Uhler - Paris: UNESCO, 2003;  
<http://unesdoc.unesco.org/images/0012/001297/129725e.pdf>



# **E-Government Projects and Their Impacts in Turkey**

**Prof. Dr. Murat Aşkar**

**[askar@eee.metu.edu.tr](mailto:askar@eee.metu.edu.tr)**

**Electrical & Electronics Engineering Department  
Middle East Technical University  
Ankara, TURKEY**

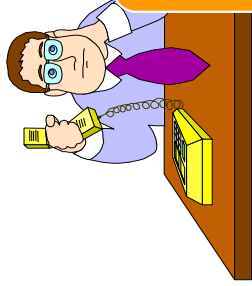
# Scope of the Presentation

- E-government (scope, models, and regulation)
- History of e-government activities in Turkey
- eEurope+ Action Plan
- Global plans
- Some e-government projects and web sites
- Problems
- Conclusions

# The scope of e-government

- Access to government data and information
  - Organization duties, statistics, notices etc.
- Access to downloadable documents and forms
  - Manual submission
- On-line services
  - Between government units/organizations
  - Direct connection to citizens
  - Indirect connection to citizens

# E-Government Model



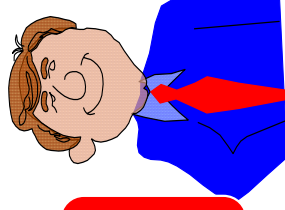
**Government  
Office**



**Government  
Office**



**Business**



**Citizen**

# The Scope of a Legal Structure

- **Mission and Administrative structure**
  - Organizational structure, responsibilities, rights etc.
- **Financial issues**
  - The income and expenditure methods
- **Personnel affairs**
  - Quality, quantity, responsibilities, rights etc.
- **Technical**
  - Interoperability problems, standards setting, testing, and certifying bodies



# History

- Higher Board of PUBLIC-NET
  - KAMU-NET Establishment: 1998
  - Headed by Undersecretariat of Prime Ministry
- Main Tasks
  - Establishment of National Government Network infrastructure
  - Coordination and monitoring the informatics projects within government organizations
  - Developing standards

# The expectations of the Public

- To find out and pay bills, tax etc 82.6 %
- To submit petition and get answers 75.5 %
- Making reservations and get tickets 73.5 %
- Exchanging information 73.2 %
- Film/music and other cultural events 73.2 %
- Participation in discussions and voting 69.6 %
- To receive diploma/certificate 66.8 %
- To reach to libraries, museums, art gal. 64.9 %
- To buy goods 62.0 %
- Bank/stock exchange transactions 58.5 %
- To apply for a job 57.2 %

## **eEurope+ Action Plan**

- **Turkey is monitoring and benchmarking the objectives in eEurope+**
  - **Accelerate the putting in place of the basic building blocks for the IS**
  - **A cheaper, faster, secure Internet**
  - **Investing in people and skills**
  - **Stimulate the use of the Internet**
    - **Government online: electronic access to public services**

## **Global plans – by the end of 2003**

- Telecom sector will be liberalized
- Special support will be given to the IS projects in underdeveloped regions
- Digital signature and legal infrastructure for e-commerce will be established
- A health telematic network will be developed, to reach to EU networks and databases will be possible

## **Global plans – by the end of 2004**

- For basic IT usage, a European wide certificate will be promoted
- The e-commerce activities will be supported with the support of private sector and consumers; to built trust, proper initiatives will be supported
- Plans for the intelligent transport services will be prepared

## **Global plans – by the end of 2006**

- All schools, students and teachers will reach to internet; course contents will be modified to be compliant with new IT technologies
- Suitable IT courses will be organized for unemployed people
- Design for all standards will be developed.
- Digital signature usage in government portals will be supported, an e-marketplace will be established for government procurements.

# Some e-government projects-1

- **Ministry of Interior:** [www.icisleri.gov.tr](http://www.icisleri.gov.tr)
  - The generation of a unique Citizenship ID Code
    - One of the most important projects; so far more than 100 million records have been entered into computer
  - Passport applications are accepted in electronic form.
- **Ministry of Justice:** [www.adalet.gov.tr](http://www.adalet.gov.tr)
  - Criminal records database is online searchable by the authorized agencies which allows fast and secure information exchange.

## Some e-government projects-2

- Ministry of Finance, Directorate General for Revenues: [www.gelirler.gov.tr](http://www.gelirler.gov.tr) (1<sup>st</sup> prize-2002)
  - Query of tax and ownership related information for transport vehicles on the Internet in addition to the traffic fines and tax identification numbers.
- Ministry of Health: [www.saglik.gov.tr](http://www.saglik.gov.tr)
  - A telematic network is in the pilot phase and allows information exchange between primary and secondary healthcare providers.



## Some e-government projects-3

- Central Bank of Republic of Turkey:  
[www.tcmb.gov.tr](http://www.tcmb.gov.tr) (**Special prize-2002**)
  - Electronic Fund Transfer System, Electronic Data Interchange System and Electronic Data Distribution System allow provision of online information dissemination in financial sector.
  - Government bonds are sold online through branches of Central Bank.

## Some e-government projects-4

- **Undersecretariat of Customs:**  
[www.gumruk.gov.tr](http://www.gumruk.gov.tr)
  - All the customs related procedures can be carried out online through “Modernization of Customs” project.
- **Directorate General of National Property:**  
[www.milliemlak.gov.tr](http://www.milliemlak.gov.tr)
  - Sale and rent announcements for real estates owned by the government are published on the Internet.

## Some e-government projects-5

- Directorate General of Rural Services:  
[www.khgm.gov.tr](http://www.khgm.gov.tr)
  - “Rural and Agricultural Infrastructure Database” is available on the Internet.
- Social Security Agency: [www.ssk.gov.tr](http://www.ssk.gov.tr)
  - The pensioners’ payment records are searchable via Internet.

# Some e-government projects-6

- Directorate General of Pension Fund:  
[www.emekli.gov.tr](http://www.emekli.gov.tr)  
**(2<sup>nd</sup> prize in 2002 and 2003)**
  - Approval of retirement applications, combination of different services and bank payment payroll procedures conducted via Internet.
  - Medical services project allows the Pension Fund to communicate with the pharmacies, hospitals and opticians electronically.

# Some e-government projects-7

- **Capital Markets Board: [www.spk.gov.tr](http://www.spk.gov.tr)**
  - Intermediary institutions are capable of gathering stock orders via electronic means including Internet.
  - Market data are published electronically via data distribution system and data distribution institutions.
  - Settlement and Custody Data Bank records are searchable online.

## Some e-government projects-8

- **State Equipment Supply Office:**  
[www.dmo.gov.tr](http://www.dmo.gov.tr)
  - “Electronic Commerce Project” allows the buyers to surf through the “Virtual Catalog” and submit the orders. The site includes also “Annual Requirement Programme” and tender announcements.

# Some e-government projects-9

- Government - Banking applications
  - Telephone bills (Turk Telecom)
  - Income tax, vehicle tax (Min. of Finance)
  - Traffic fine (Min. of Finance)
  - Social security premium (Min. of Labor and Social Security)

# Some e-government projects-10

- Other Banking projects
  - Electricity, water bills (municipalities)
  - University fees (Universities)

Most of these applications,  
are not on-line.



## Other Government Sites

- General Directorate of Security
  - POLNET (Best Site Prize - 2003)
- General Directorate of Pension Fund
  - Control of Health Expenses (2nd bestprize-2003)
- Ministry of Education
  - Integrated Management Information System
- Ministry of Industry and Trade
  - SANAYI-NET (Industry – net)

# Some Municipality Sites

- Istanbul Kadikoy Municipality
  - Municipality Management Services (1st prize 2003)
- Istanbul Metropolitan Municipality Internet
  - Office of Water and Sewerage Admin. (2nd prize in 2003)
- Eskisehir Metropolitan Municipality
  - eEskisehir (e-city)
- Istanbul Besiktas Municipality
  - eDonusum (e-transformation)

# Problems

Problems to set up a real on-line e-government environment:

- Legal issues
- Infrastructural and human resources issues
- Financial and Administrative issues

# Legal issues

- Digital signature law
- Protection of personal data
- Legislation on internet crimes
- Protection of Consumer Rights
- State Procurement Law
- Lack of Standards
- Legislation on Electronic Agreements

## **Infrastructural and Human Resources Issues**

- **Speed of the internet (Liberation of TT)**
- **Limited hardware and software**
- **Incompatible data base structures**
- **Inappropriate software**
- **Lack of back-up systems**
- **Shortage of qualified personnel**
- **Lack of professional training**
- **Lack of public kiosks (internet cafes)**

# **Financial and Administrative Issues**

- Improper project descriptions
- Underestimated project costs
- Delayed or unfinished projects
- High maintenance costs
- Training the old citizens

# Conclusions - 1

- Almost all government organizations have web sites
- Citizens can get information about government activities, reach to all legal documents
- Citizens can download docs and forms.
- Internet banking related with government payments is rapidly increasing
- The usage of the system by old citizens is still a problem

## Conclusions - 2

- We are at the very beginning of e-government world, however we should support different applications.
  - A legal framework may be needed for the misuse of multi-identity case!
- A proper legal environment will enhance the usage of these applications
  - Digital signature law may not be sufficient
  - Who will certify the tools that the citizens are using (browsers, smart cards etc.)





E - g o v e r n a n c e  
**Academy**

**Access to Information as the  
foundation of e-Government: the  
case of Estonia**

**Ivar Tallo**  
Director of e-Governance Academy

# Plan of the presentation

- **Some theoretical moments**
- **Practical examples of access to information in Estonia**
- **Conclusions**

# Theory

- **4 stages to build an e-government ...**
  - One way communication: information provision via web-pages
  - Two way communication: e-mails, downloading blank documents
  - Interaction: paying taxes on-line
  - Integrated service provision: e.g. citizen portals
  - (Integrated e-governance: shaping policies)
- **Regulation of information flows:**
  - Anglo-American
  - Continental European
  - Scandinavian

## Functional vs. normative

- Access to information (freedom of information) as a demand for a democratic governance
- Access to information as a foundation for more effective government
- Information “*just in case*” vs. “*information on demand*”

**Just to remind you ....  
We are a very small country  
in a cold Nordic neighborhood!**



Potsdam, November 11th, 2003



## Why Estonia:

- Internet penetration 45% as of May 2003
- One of the top countries in developed e-government: 5<sup>th</sup> place in the Harward Networked Readyness e-government subindex
- 9<sup>th</sup> place in online environment (World Competitiveness Yearbook 2001)
- Among top ten countries in terms of e-readyness (according to McConnell International)
- One of the leading countries in PIAP next to Finland and Canada
- 2.35 DSL connections per 100 – 16<sup>th</sup> place in the world
- But 42<sup>th</sup> in Human Development Index (UNDP)
- GDP per person 1/3 of the EU average

## **Estonian Public Information Law**

- **Constitution §44: all public information shall be open ...**
- **Demand for an “active information provision”**
- **Digital document registries**
- **Definition of information that cannot be restricted**
- **Requirement for all public institutions to have a home page.**
- **Requirement for all public libraries to have a public internet access point**



## **A holder of information is required to disclose the following existing information relating to the duties thereof:**

- 1) generalised economic statistics and economic forecasts of the state and local governments;
- 2) generalised statistics relating to crime and misdemeanours;
- 3) statutes of state or local government agencies and their structural units;
- 4) formats of petitions and other documents submitted to state and local government agencies and instructions for the completion thereof;
- 5) job descriptions of state and local government officials;
- 6) positions in state and local government agencies, and the given names, surnames, education, areas of specialisation, telephone numbers and electronic mail addresses of officials filling the positions prescribed in such agencies;
- 7) information concerning danger to the life, health and property of persons;
- 8) reports on work results and the performance of duties in state and local government agencies;
- 9) names and electronic mail addresses of members of the supervisory boards and management boards of legal persons in public law;
- 10) management reports and income and expense statements of legal persons in public law;
- 11) budgets and draft budgets of state agencies, local governments and local government agencies, and reports on the implementation thereof;

## **Information provision**

- **Separate web-pages for all institutions functioning under the public law**
- **Integrated e-government portal to access information**
  - E-briefing room
  - E-state gazette
  - TOM
- **Integrated e-citizen portal to access information and communicate with government**
  - Possibility to check and correct personal information
  - Possibility to apply for services on-line

# X-road and citizen information

- [www.riik.ee](http://www.riik.ee) – the central government portal
- [www.riso.ee](http://www.riso.ee) – back door to x-road, home page of the Department of Estonian State Information Systems

# Conclusion

- **Easy access to public information is both question of democratic governance and efficient state administration**
- **It is possible to take the current administrative procedures into the net but the real gains in efficiency come only when we change administrative procedures and start from the premise of public information being public.**

## **Couple of words about the future ...**

- **The future of e-government is m-government**
- **An explosive growth of WIFI**
- **M-information**
- **M-beer**
- **M-parking**
- **M-payments (ca 1000 vendors)**
- **M-police – an integrated internal safety concept**



E - g o v e r n a n c e  
**Academy**

**Thank you for your attention!**

Questions: [ivar.tallo@ega.ee](mailto:ivar.tallo@ega.ee)



## **Jernej Rovšek**

Deputy Human Rights Ombudsman  
and Independent Commissioner for Data Protection,  
Ljubljana, Slovenia

# **Freedom of Information and the E-Government projects in the Republic of Slovenia**

## **I. Introduction**

This contribution is an attempt to present the state of affairs and certain projects in the area of access to information of a public nature and of the development of e-government in Slovenia. These two topics are linked, since they also derive from the right of the individual to be familiarised with the functioning of public administration, which within the framework of democratic processes facilitates the influence and control of the citizens over the public administration's work. They are also linked to the right of the individual to privacy, since the development of information technologies and e-commerce offers greater scope for collecting, processing and linking up data, and in this way they pose the constant threat of unjustified use and disclosure of personal data.

Alongside other areas, these issues are also addressed by the Human Rights Ombudsman, the national ombudsman with the broadest powers, who oversees the entire domain of public administration. The Slovenian ombudsman has full authorisation to perform informal oversight of all state bodies, local community bodies and also of private subjects, although only when they are carrying out public authorisations. With the amendments to the Personal Data Protection Act in 2001, the ombudsman acquired new tasks as the independent data protection supervisory institution. Within this institution, and as a deputy ombudsman, I cover also certain of the aforementioned areas, so this presentation will be primarily from the aspect of ombudsman assignments, namely assisting individuals in exercising their rights in relation to public administration.



## II. Transparency and public nature of public administration

### 1. Proposals and activities of the Human Rights Ombudsman

It may be said that in Slovenia, it was precisely the ombudsman who first publicly, and with some determination, raised the issue of transparency in the functioning of public administration institutions. Within this framework, an especially important contribution was made in the ombudsman's annual report for 1998, which was published in April 1999 (it is accessible at [www.varuh-rs.si](http://www.varuh-rs.si)). A special analysis in the introductory section of this report focused on issues of access to information of a public nature, and this generated a wide response in debates in both houses of parliament and also in the public.

This analysis began by emphasising that the right to obtain information of a public nature, as guaranteed by the provision of Article 39 of the 1991 Constitution, is one of the latest constitutional human rights that has not been rendered operational in law and is therefore hard to fulfil in practice. The Constitution requires legal provision to be made for the fulfilment of this right, since the law must lay down exceptions regarding access, and must prescribe the procedure for exercising this right. The ombudsman's first proposal was that the government should at the earliest opportunity draft a law that would regulate the method of exercising this constitutional right. We also proposed that a fundamental law on the confidentiality of data in state bodies be adopted, since this area had been covered by various regulations, including implementing regulations, and that they study the setting up of a special body that would be concerned informally and non-judicially with fulfilment of the right of access to information (a special information technology ombudsman). At the same time we recommended to all bodies of public administration that, despite the legal vacuum, they enable access to information in their domain for individuals and adopt their own internal rules about this.

Alongside the demand for a legal framework for access to public information, in this analysis the ombudsman offered suggestions for regulating three other areas that are linked to transparency in the functioning of public administration. Firstly we made a critical assessment of the area of **free access to regulations**. At that time

the revised wording of regulations was only accessible via a commercial provider. We assessed this situation as being unacceptable, and suggested that all state bodies should provide free access to all national and local regulations, particularly via the Internet. This part of the recommendations also attracted considerable attention, and we observed that following the publication of these suggestions, the situation changed significantly. The public company that issues official publications (Official Gazette) now enables free access on the Internet to all publications, except for advertisements and tenders, from 1995 on. The National Assembly and the Government now also provide free access on their websites both to adopted regulations and to those that are being deliberated, along with their explanatory material. Access is also provided to other parliamentary material, including all literal transcripts of parliamentary sessions. The government started publishing a free register of regulations, which provides a basis for rapid searching of regulations being sought. There was less success in carrying out our suggestion that a standardised register of local community regulations should also be provided.

Following the adoption of our suggestions, major progress was achieved in the **accessibility of jurisprudence**. Slovenia's Constitutional Court and Supreme Court now enable access to their case-law in the full wording on their respective websites. However, case-law of the lower courts is still only accessible via commercial providers of legal information.

In the 1998 report the ombudsman also proposed the more active role of state bodies in **publishing information on the worldwide web**. We proposed that in addition to publishing regulations within their own domains, state bodies **include professional circles and NGO-s in the process of drafting implementing regulations**, and that they adopt their own rules about this. Given the importance of transparency in complaints procedures, we suggested in particular that all public administration bodies should provide **information about complaints procedures** within their domain.

The final area that we analysed involves **access to information on environmental protection**. It is precisely in the area of environmental protection that transparency of operations and the possibility of rapid access to information on environmental pollution are particularly important. The 1993 Environmental Protection Act

ticularly important. The 1993 Environmental Protection Act contains in our opinion inadequate and vague rules on access to environmental information, since it allows for differing interpretations. We determined this on the basis of our own research and information communicated to us by non-governmental organisations. We suggested that the government ratify as soon as possible the Aarhus Convention, which contains more precise rules on access to environmental information than the 1993 Act. We proposed the earlier implementation of the Aarhus Convention, so that wherever the Act does not provide a solution, public administration bodies could directly apply the provisions of the Convention. Despite numerous assurances from the government, and recommendations from the ombudsman, Slovenian Parliament has still not ratified Aarhus Convention.

These suggestions contained in the annual report generated a response in the National Assembly, which passed decisions proposing fulfilment of a number of the ombudsman's suggestions. Those suggestions that were not put into effect were repeated in annual reports in subsequent years. Nevertheless, we have observed that the ombudsman's proposals and suggestions have had a major impact in favour of a more rapid opening up and greater transparency in the functioning of public administration.

## **2. Adoption of regulations on the transparency of public administration**

To begin with, the **Confidential Data Act** was adopted in 2001, and this now provides in one place the rules regarding which data, for various reasons, should be defined as confidential. This effected a major advance in demarcating information accessible to the public, and information which in a lawfully provided manner is not publicly accessible.

The most important step was the adoption of the **Act on Access to Information of Public Character** in March 2003. Non-governmental organisations and the ombudsman wielded considerable influence in the adoption of this act. Together we drew up a legal project which, although it was not formally submitted for legislative procedure, had major influence on the wording of the adopted Act proposed by the government. Through the coalition of non-governmen-

tal organisations, which had organised themselves especially for this project, I also participated personally in the preparation of this project, and also in the reading of the government's bill in parliament.

Viewed in its entirety, the adopted act is up to date and contains criteria for access to public information that are contemporary and open, also in comparison to most developed European countries in this respect. The non-governmental organisations, which were joined by the Human Rights Ombudsman, had the most remarks and reservations about the mechanisms of oversight and incentive in implementing the act. They proposed a special information ombudsman, who would be incorporated into the existing ombudsman institution. This proposal was not adopted, but in its place a special plenipotentiary was established by law, and while this authority has a high and independent position, its powers are restricted to issuing decisions on second-instance administrative appeals, and it has no role of providing incentives or guidance in implementing the Act. This role was entrusted by law to the Ministry of the Information Society. Our view is that this solution is not good. Access to information of a public nature is primarily the right of citizens, so we therefore took the view that it would be more appropriate to authorise a special independent body (special ombudsman) for this task, or to leave it to NGO-s.

The act introduces numerous new and demanding obligations for public administration bodies. They must set up catalogues of all public data and publish them. All bodies must also identify one or more official persons who are especially responsible for the dissemination of information and for conducting the procedure upon request. The procedure must be conducted in compliance with the act governing general administrative procedure. They must decide on requests for access within 20 working days. In our assessment this deadline is too long, since much information has a very short useful lifetime. In the event of a denial of request, bodies must issue an administrative decision. The appeals body of second instance is, as stated, the special authority; and the procedure may be continued against this authority's decision at the administrative court. All public administration bodies must adopt internal rules on conducting the procedure, they must adopt and publish a list of tariffs (they can charge only for the material costs of providing information) and each

year by the end of January they must draw up an annual report on implementation of the act and submit it to the government, which in turn draws up a common annual report for parliament and publishes it on the Internet.

This act will most certainly have a great influence on the development of information technology within public administration bodies and on e-government projects. Article 10 of the act sets out the information that each public body is bound to publish on the Internet. This comprises the revised wording of regulations, linked to the national registry of regulations; programmes, strategies, analyses and studies; proposed regulations and other documents relating to the area of the individual public administration body; all tenders and public procurements; data on administrative services for citizens and other information of a public nature.

The implementing regulations that are being drafted on the basis of this act also envisage the Internet publication of the drafts of all official acts and other documents that bodies intend to adopt, at least two or four weeks prior to their adoption, in order to allow for public and expert debate.

### **III. E-government achievements and projects in Slovenia**

In this second part I shall offer a brief presentation of the achievements and plans in developing e-government in the Republic of Slovenia. For assistance in obtaining this information I thank the director of the Government Centre for Informatics, who furnished me with the latest data on e-government projects in Slovenia.

We understand the term e-government as a programme of numerous projects in the area of electronic operations in public administration. This therefore involves projects within the administration and also projects of operations between citizens and the administration and economic subjects and the administration.

One milestone in the development of e-government is the Strategy of e-commerce for Public Administration for the period 2001 to 2004, which was adopted by the Slovenian government in February 2001. Certain supporting activities had in fact already been carried

out earlier. Apart from the gradual introduction of IT in the state administration, the most important element was adoption of the legal foundations for implementing e-business in public administration. Foremost of these are: the Electronic Commerce and Electronic Signature Act of 2001, and its associated implementing regulation on the criteria for e-administration and e-signatures; the Personal Data Protection Act, General Administrative Procedure Act and Administrative Taxes Act. The main objectives of the strategy are: accelerating the implementation of electronic services, greater coordination between individual bodies, consolidation and connectability of registers and records, rationalisation of business in public administration and faster and friendlier services for citizens. Another objective is greater transparency of service in public administration, and comparability with the standards in other European countries.

## 1. Projects aimed at citizens

For more than two years now the **national e-government portal** (<http://e-gov.gov.si/e-uprava>) has been in operation. This provides a standardised entry point to various areas of public administration, and links up to different public administration bodies. The portal allows access by subject groups to state bodies and their services, and in addition to basic information on the functioning and services of public administration it offers to the state and citizens individual specific e-services. The portal, which also allows individual customisation, is visited by around 5,000 users per day.

In 2003 a new **territorial administrative units portal** came into being, and is aimed at making it easier for citizens to perform often too lengthy services at administrative units. The citizens' guide describes practically all the administrative procedures through various life situations. The portal supports standardised forms in several languages used in Slovenia to obtain various certificates, copies, decisions and other administrative services for residents. This portal is visited by an average of 2,000 users per day.

The first proper e-service for citizens is the **electronic application for obtaining a copy from the Central register of inhabitants (CRI)**, which can be accessed by those who hold digital certificate authenticated by the official verification service (SIGEM-CA). To date a total of 7,000 certificates have been issued, and around 700

applications for copies from CRI have been received, processed and fulfilled.

The most recent acquisition for e-government in 2003 has been the **possibility of citizens accessing their own personal data in the CRI**. Citizens who have digital certificate can review all current information, as well as the history of events up to 1980. The purpose of this service is to enable citizens to exercise their constitutional right to be familiarised with their own personal data and the possibility of correcting this, something regulated in detail by the Personal Data Protection Act.

For several years now there have been plans to set up the possibility of sending in **tax returns** by e-mail. Owing to the lack of success in public tenders for this project, it is still not available, and this has caused some dissatisfaction among the public. Fulfilment of this project is also planned for the near future.

## **2. Projects within the state administration**

Of the projects intended to provide easier and faster linking of data between different records within the state administration, mention should be made of the project to **link the central CRI records to the Pensions and Disability Insurance Agency**. Currently this institute has direct access to the central database of citizens who are claiming rights at the Agency. In this way, in one year more than 50,000 direct searches in the CRI were carried out. This means that this same number of citizens did not need to bring in their own confirmations from administrative units.

There has also been success in carrying out the project of **linking administrative units and social work centres with the CRI**, which has enabled faster and more accurate acquisition of data needed by citizens to fulfil their demands in the area of social benefits. In this way both citizens and state officials make savings, since there is no need for the traditional method of gathering basic information on the persons whose applications are being dealt with.

### **3. Projects aimed at the commercial sector**

In this area the development of e-commerce in Slovenia is lagging behind more than in other areas, compared to other European countries. The first electronic service was the e-book of decisions for commercial companies that must be confirmed by a notary. This project includes all the notaries in the territory of Slovenia, and currently 5,700 companies, but at the moment books of decisions are being kept entirely in electronic form for 30 companies.

### **4. E-voting project**

The Government Centre for Informatics has determined that in Slovenia all the technological requirements have been met for conducting electronic voting. This year the government submitted a proposed revision of the Elections Act to the National Assembly, where it proposes enshrining e-voting in law. However, the first reactions of government coalition parties have been reserved, with some being concerned about the possibilities for overseeing the conducting of such voting, so there is a question mark over this possibility being exercised for the next parliamentary elections in 2004.

### **5. Other projects and future plans**

A new portal is being prepared in the state administration, and this will be geared more towards individual target groups of citizens. This year should see the creation of the e-employment project, which will enable holders of a digital certificate to access the exchange of data between those offering and seeking employment.

There are plans to incorporate new public administration bodies into the CRI, such as the health and employment institutes, municipalities, courts, national archives and others. There are also plans for a project of electronic tax payments, covering the payment of income tax and other tax. And although great transparency has already been established in the area of public procurement, new forms of carrying out public e-procurement are planned.



## **IV. Conclusion**

In the area of transparency in the functioning of public administration and development of e-government, great progress has been made in Slovenia in recent years. All the main regulations facilitating the rapid development of this area have been adopted. The research carried out by the government's IT office this year shows that on average Slovenia still lags behind the EU countries and Iceland, Norway and Switzerland (from the Web-based Survey on Electronic Services) by 13 percentage points, with Slovenia actually being more advanced than the EU average in services for citizens, but showing a lower ranking in the overall picture by lagging behind in services for companies. Meanwhile, given the rapid development, new questions are being raised about the effectiveness of privacy protection, although this is a different subject that would require separate presentation.

Ljubljana, September 2003

**eGovernment - across the boarders.  
How to act - not just talk about.**

**"Cities on Internet" Association  
approach"**



**© Stowarzyszenie  
"Miasta w Internecie"**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# How to manage the eGovernment in such a country like Poland?

- ❑ 38 million of inhabitants
- ❑ 16 regions – 1,5 - 3,5 mln of inhabitants [NUTS II], Wielkopolska Region – 3,4 mln, [Lithuania – 3.5, Latvia – 2.3 Estonia – 1.4, Slovenia – 1.9, Hungary - 10,1, Czech Republic –10,2, Slovakia 5,4, Malta – 0,4, Cyprus - 0,8]
- ❑ quite weak position [small budget for investments] of regional authorities so far
- ❑ centralised IT infrastructure built in 80' and 90':
  - ✓ national register of citizens – PESEL
  - ✓ national register of tax payers – NIP
  - ✓ national register of self - employers and companies – REGON
  - ✓ lack of central government back office integration
- ❑ strong legal position of local authorities, but their budgetal weakness
  - ✓ almost all public services delivered by local authorities



© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# eGovernment backwardness in Poland? Challenges to face!

## Germany

### Strategies/ Programmes/

- *Bund on line 2005*
- numerous regional and local information society strategies and masterplans in the implementation phase

### Management

- Ministry of Interior [Bund on line 2005]
- Ministry of Economic and Labour [MEDIA@KOMM]

## Poland

- lack of eGov strategy on the national level
- Silesia Region, Malopolska Region are working on Information Society strategies, City of Gdańsk adopted the IS strategy, some cities - like - Wroclaw are considering to do it
- lack of clear leadership - some ministries play the traditional parts: Ministry of Interior [registers, personal documents], Ministry of Economy, Labour and Sociela Policy [IREP with IS component], Ministry of Science and Informatisation [should co-ordinate, but so far NO legal/financial basisto do that]



© Stowarzyszenie  
“Miasta w Internecie”

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# eGovernment backwardness in Poland? Challenges to face! [2]

## Germany

- Standardisation towards interoperability and security
  - SAGA - OSCI
- Dedicated budget
  - YES
- Regional projects
  - Several financial models/sources
    - governmental budgets
    - PPP
    - structural funds
    - INTERREG
    - Innovative actions
- Awareness of public sector employees
  - Relatively HIGH from EU perspective

## Poland

- lack on the central and local level [lack of concrete central government activities so far]
- in general - NO, some exceptions
- 2 regional „gateways” of Malopolska [after 2 years of development} and Podlasie [starting phase] regions - central governmental support
- lack of support from SF, INTERREG, innovative actions
- Very LOW on both fields: regional/policy implementation and eGovernment



© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

## Regulatory framework on access to information

- Act on Protection of Personal Data (1997)
  - ✓ Establishment of the Inspector General of Poland for protection of personal data
- Act of confidential information (1999 with further corrections)
- Act on Access to Public Information (2001)



© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# Citizens access to public information

- Legal base:
  - ✓ Article 61 of Constitution of Republic of Poland - citizens right to access to public information
  - ✓ Access to Public Information Act
- Request to public entities obligation to provide citizens with PI
  - ✓ obligation to pay of cost for copying, printing “heavy docs” and CD
  - ✓ administrative procedure to get the information [14 days for response]
- Public Information Bulletin
  - ✓ Public Information Act, 6th September 2001 (Dz.U. 2001 Nr 112, poz. 1198),
  - ✓ Decree of Minister of Interior and Public Administration, 17th May 2002, about Public Information Bulletin (Dz.U. 2002 Nr 67, poz. 619).



# Public Information Bulletin

- ❑ separate web site create by every public entity, including central/ regional/ local governments and their subsidiary institutions
- ❑ data based repository of informations and documents, also some personal information of elected authorities [f.i. yearly personal tax raports]
- ❑ access 7days/24hours
- ❑ obligation to create the PIB of each entity - since VII 2003
- ❑ obligation to show on line the status of the citizens case in the particular local government - since I 2004
- ❑ obligation to show on line the GIS based information on line - since I 2005



© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003



# Public Information Bulletin

Obligation to open the on line access to public information - all documents and content regarding:

- ❑ internal and foreign government policies and activities,
- ❑ all public organizations including their structure, charter and property,
- ❑ information on proceedings of a government agency including legal regulations, planning and management decisions (e.g. public procurement),
- ❑ information on public properties managed by respective government agencies,
- ❑ minutes of proceedings of all elected government organs.

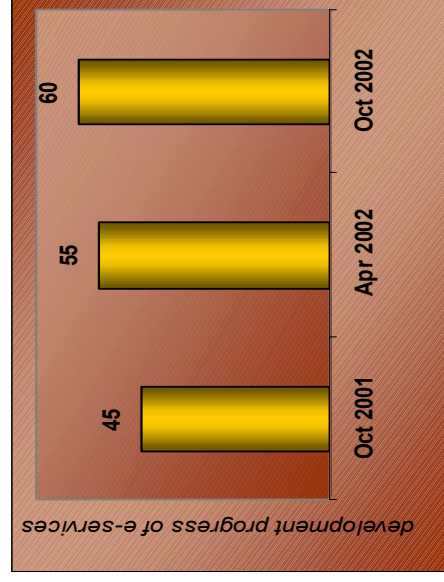
**75 % of entities didn't meet legal requirements so far**



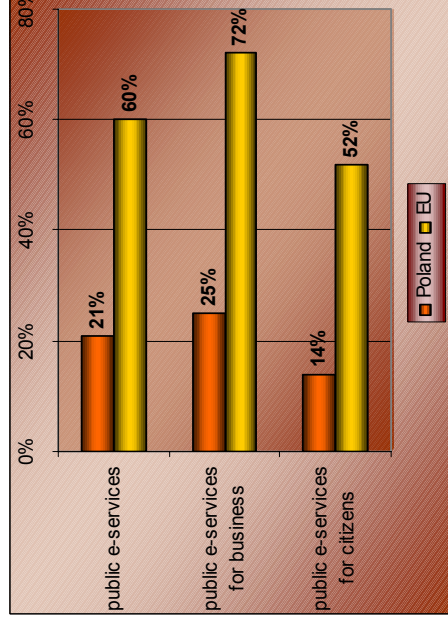
© **Stowarzyszenie**  
**“Miasta w Internecie”**

# Services for citizens [CGEY survey]

## Poland - slowest step forward among AC



Progress in European Union



EU in comparison with Poland

**Average: 21 %, services for citizens - 14%**



© Stowarzyszenie  
"Miasta w Internecie"

Transparency and E-Government in Central and Eastern Europe  
Potsdam, 11. November 2003

# Regional IS indicators



Indicators	Wielkopolska Region	Lubuskie region	Zachodnio-pomorskie region	Poland	UE
I, g web sites (2003)	65,9%	72,28%	80%	69,7%	-
Schools with comp, lab, (2002)	65,8%	63,9%	68,1%	63,1%	-
Students per one comp, [all schools] (2002)	30	26	30	30	9,2
St./comp with Internet [secondary schools] (2002)	39	34	38	26,1	14,9
Expenditures for research and development [mln PLN] - 2001	345,2	17,9	64,0	4 858,1	-
Employment in RD sektor - 2001	11696	1380	3727	123 840	-
Access to Internet	19,09%	23,06%	13,84%	20,76%	51%



# Barriers vs Strengths

-

- Lack of sectoral policy on the national level and coherent regional eGovernment strategies
- Budget limitations - eGov is NOT a distinguished part of budgets
- Low level of reflection on e-Development processes in administrations
- the approach of COMPU - and INFOR - matisation of administration versus eGovernment services
- Lack of legal regulations on public private partnership
- Low number of twinning projects implemented so far by Polish regions with its counterparts from EU

+

- Strong demographic potential
- Structural funds - eligibility (all Polish regions under Objective 1)
- e- Government area is not determined so far [projects to define]
- Strong potential of Polish ICT firms
- experiences from Framework Programme and Phare Programme

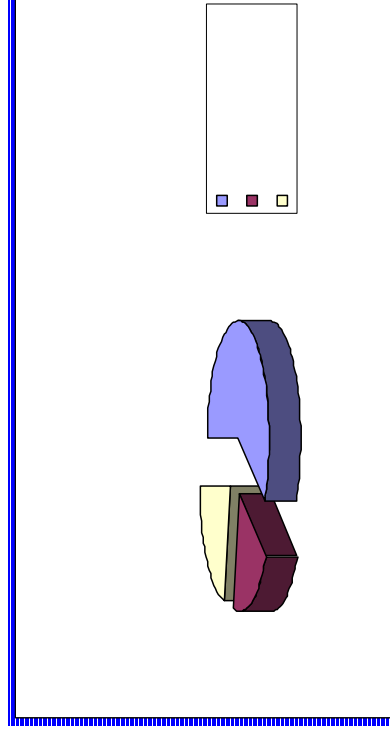


© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# Opportunities to finance of eGov projects

Activity	IROP - Integrated Regional Operational Programme			
	Total cost	Structural Funds	National contributions (state budget + l.g. budgets)	Private contributions
1.5. Information Society Infrastructure	140,00*	82,5	27,5	30,00



\* Tbc September 2003 round of negotiations



© Stowarzyszenie  
"Miasta w Internecie"

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# Knowledge Government on horizon..?

## Realistic overview

### Perspective of the year 2006

- ❑ implementation of **structural/ regional policy** - linked to general national priorities, but based on the regional needs, potentials, strategies.
- ❑ some **regions** challenge the use eGovernment solutions as the MOTOR of development in general
- ❑ some **cities** decide to create and implement the information society driven strategy
- ❑ on the national level - the financial and regulatory framework **unclear**:
  - the parliament regulation on the „informatisation of public sector” will be discussed until the **2005**
  - lack of central government co-ordinated activities towards creation of interoperability, data exchange and security standards in European sense [**late 2005?**]
  - regulation on digital signature should be implemented since **VIII 2006**, but there is no governmental programme [including financial support] to support l+r government on that field
  - some obligations resulting from „freedom of information” act to present several sets of governmental data on line
    - **1.01.2004** - state of the citizens case considered by local governments
    - **1.01.2005** - digital data in GIS systems



# Conclusions as the base for international co - operation

## International projects:

- ❑ need for “political umbrella” - the new inter - governmental initiatives on the national level [f.i. Polish-German] to facilitate the independent co-operation on the regional and local level
- ❑ use of new and existing opportunities:
  - ✓ use of existing „twinning agreements” between regions to start with eGov initiatives
  - ✓ INTERREG projects
  - ✓ 6 Framework Programme projects - 3° call, IV- IX 2004
  - ✓ support of independent foundations and IT sector players
- ❑ support of current EU regions to implement the structural policy as the motor of eGovernment implementation on the national level



# Potencial initiatives of cross-boarder co-operation between regions in Germany and Poland

- ÜBER GRENZEN HINWEG - eGovernment in strukturschwachen Regionen“
  - ✓ organised by Alcatel SEL Stiftung für Kommunikationsforschung, Hochschulkolleg E-Government der Alcatel SEL Stiftung, Heinrich-Böll-Stiftung Brandenburg - Heinrich-Böll-Stiftung and Stowarzyszenie „Miasta w Internecie“ {cities on Internet Ass.}, Tarnow, Poland
  - ✓ 3 workshops, first in Postdam on the 13th of November
- Prelude project [<http://www.elanet.org>] clusters of innovation
- Polish-German Seminar at the 8<sup>th</sup> eGovernment - Cities on Internet Conference in Zakopane, 17th of June, 2004
- Land Nordrhein - Westfalen and Silesia Voivodship co-operation [?]



© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003



# Thank you for your attention!

Krzysztof Glomb

President of „Cities on Internet Association

[k.glomb@mwi.pl](mailto:k.glomb@mwi.pl)



© **Stowarzyszenie**  
**“Miasta w Internecie”**

Transparency and E-Government in Central  
and Eastern Europe  
Potsdam, 11. November 2003

# **Geoinformationssysteme und Informationszugang**

**Referent: Franz Blaser**

# Geoinformationssysteme ...

- Was sind Geoinformationen?
- Welche Bedeutung und Nutzen haben Geoinformationen?
- Welche Potentiale beinhaltet der Geoinformationsmarkt?
- Für welche Anwendungen werden Geoinformationen heute schon nachgefragt?
- Produktionsstufen am Geoinformationsmarkt
- Wie sieht die Produktpalette der Geodatenanbieter aus?

## ... und Informationszugang

- Wie kommt man zu Geoinformationen?
- Was behindert zur Zeit noch den Zugang zu Geoinformationen?
- Wie sehen die Konzepte für einen besseren Zugang zu Geoinformationen aus?
- Geoinformationen im Spannungsfeld
  - Datenschutz und Urheberrecht
  - Informationsfreiheit und Umweltinformationen

# Was sind Geoinformationen? (1)

- Geoinformationen:  
sind Informationen über Objekte mit Raumbezug
- Geodaten:  
sind rechnerlesbare Geoinformationen
- Geobasisdaten:  
sind grundlegende amtliche Geodaten, welche die Landschaft (Topographie), die Grundstücke und die Gebäude anwendungsneutral in einem einheitlichen geodätischen Bezugssystem beschreiben

## Was sind Geoinformationen? (2)

- Geofachdaten:  
sind thematische Daten mit Ortsbezug, der sowohl direkt durch geographische Koordinaten als auch indirekt, z. B. durch Postleitzahlbezirk oder administrative Einheit, gegeben sein kann
- Geoinformationssystem (GIS):  
Ein IT-basiertes Informationssystem mit Funktionen zur Erfassung, Aktualisierung, Verwaltung und Analyse von Geodaten sowie zur kartographischen Darstellung von Geoinformationen

# Bedeutung und Nutzen von GI

- Ca. 80% aller Informationen im öffentlichen und privaten Leben weisen einen räumlichen Bezug auf.
- Der Einsatz von Geoinformationssystemen führt zu effektiveren Arbeitsmethoden und besser vorbereiteten Handlungsentscheidungen.
- Geoinformationen stellen ein Wirtschaftsgut von herausragender Bedeutung dar.

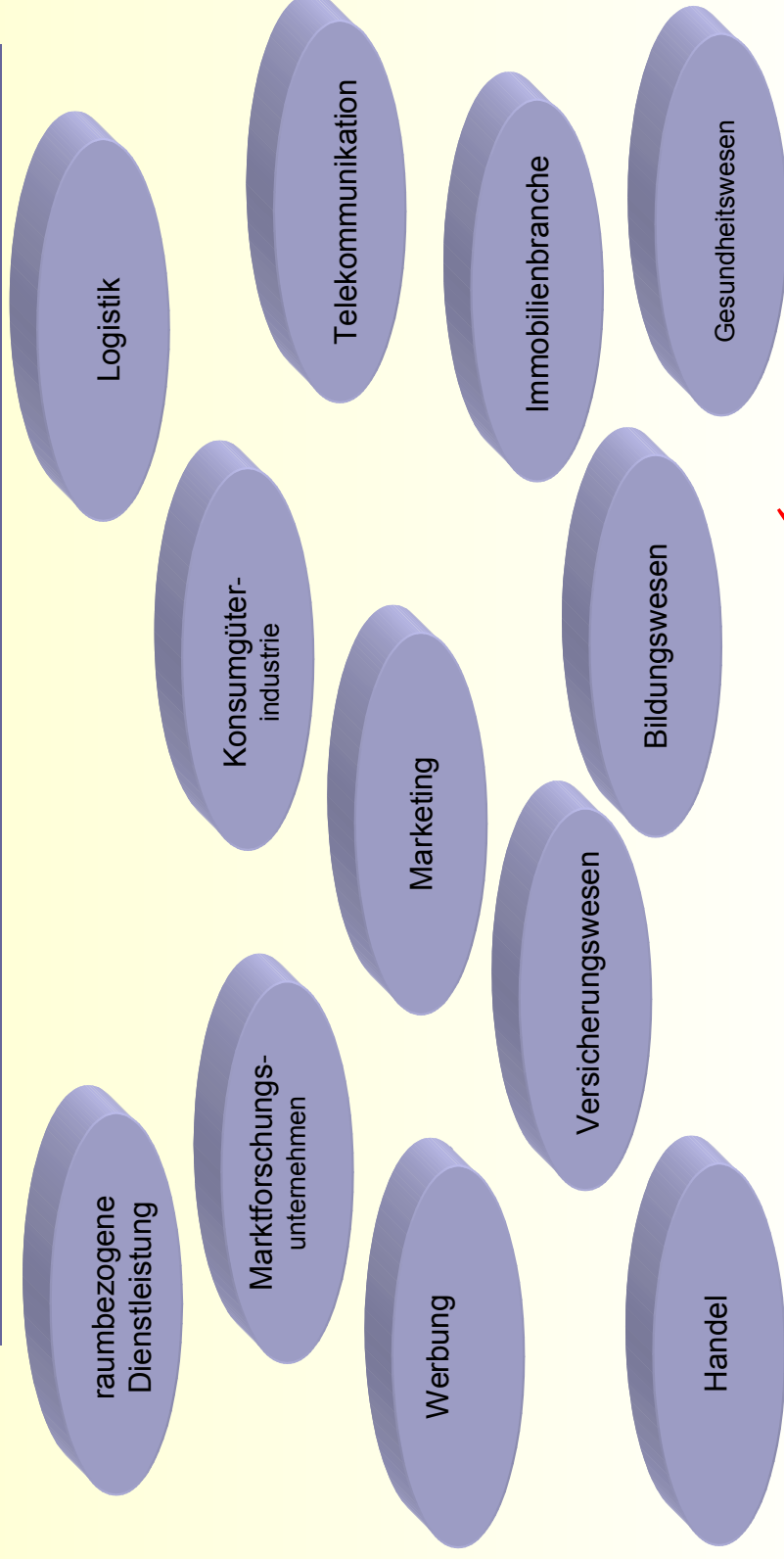
# Potentiale des GI-Marktes

## MICUS-Studie:

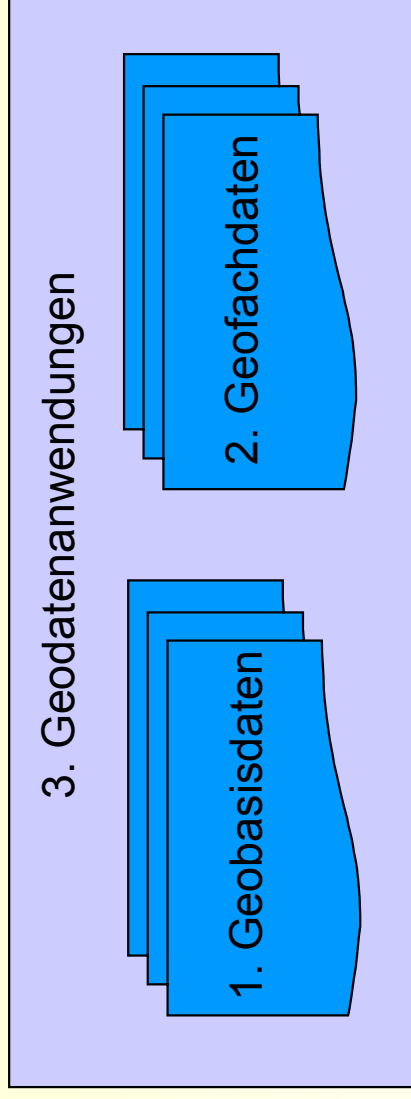
- Potential des deutschen Geoinformationsmarktes wird auf ca. 8 Mrd. € geschätzt
- z.Z. werden lediglich 15 % ausgeschöpft
- bei marktgerechter Bereitstellung von GI ist jährliches Wachstum von 10 % realistisch
- Wachstumsimpulse:
  1. Direktes Wachstum des GI-Marktes
  2. Qualitätssprung der Unternehmensplanung
  3. Verbesserung der Infrastruktur



# Potenzielle Geodatenutzer



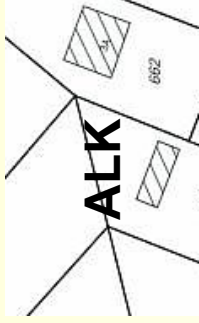
# Produktionsstufen



## Anbieter am Geoinformationsmarkt:

- Öffentliche Verwaltung
- Wirtschaft
- Wissenschaft und Forschung

# Angebote Geobasisdaten



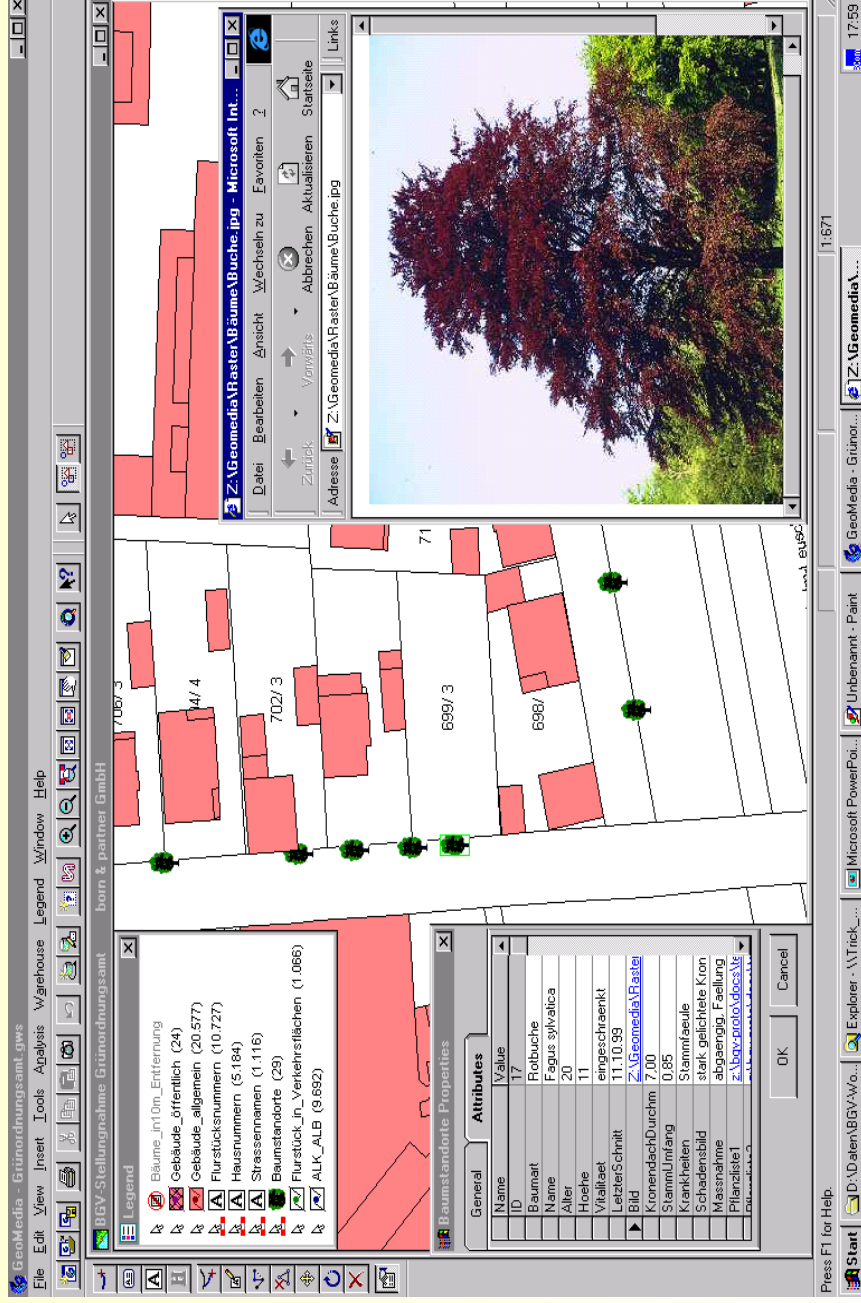
## Geobasisdaten



# Geodatenanbieter und/oder Anwendungen in der Öffentlichen Verwaltung:

- Bauleitplanung
- Geologische Karten
- Planungsinformationssystem (PLIS)
- Statistisches Jahrbuch
- Bevölkerungsdaten
- Denkmalschutz
- Wirtschaftsdaten
- Baumkataster / Grünplanung
- Wetterdienst
- Biotop- und  
Artenschutzkartierungen
- Katastrophenschutz /  
Notfallvorsorge (deNIS)
- Altlasten- u. Deponiekataster
- Wasser- und Schifffahrts-  
verwaltung (WaGIS)
- Nationalparkverwaltung
- Landwirtschafts- und Umwelt-  
informationssystem (LUIS)
- Bundestagswahlkreise  
(WEGIS)

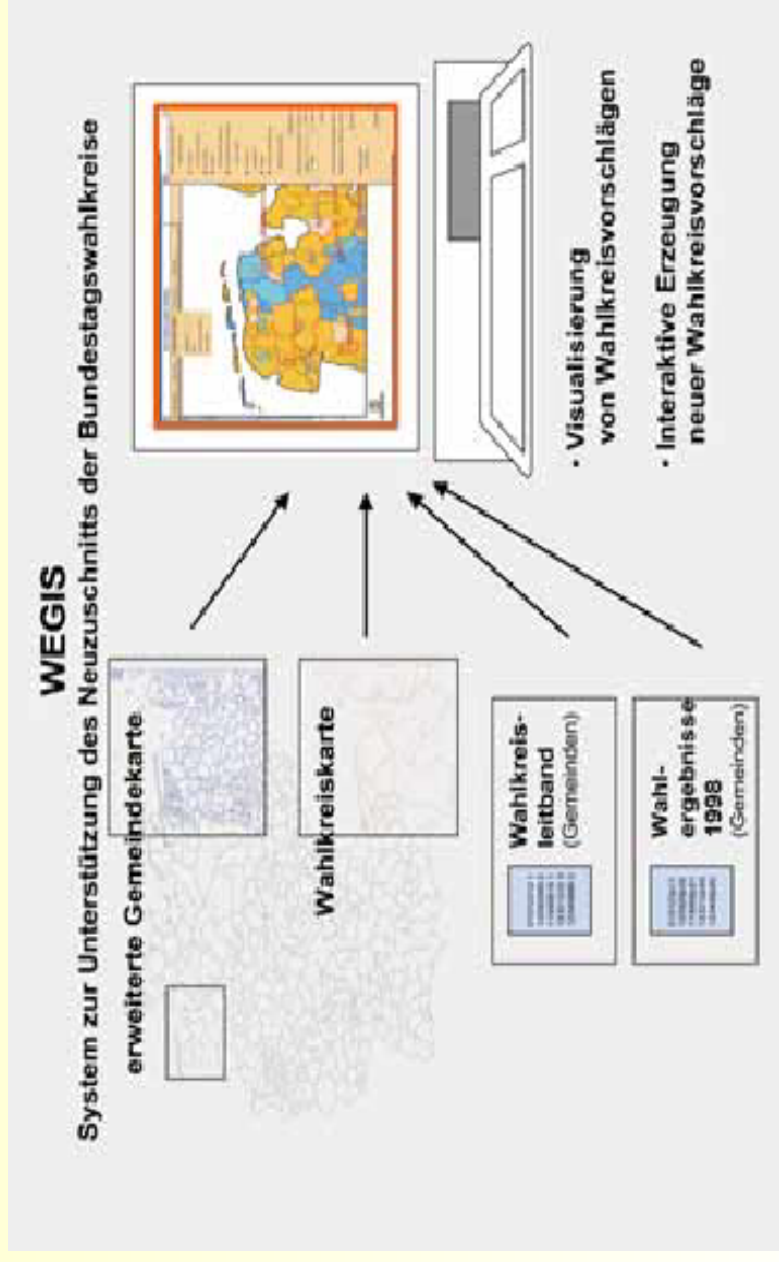
# Beispiel: Baumkataster



# GIS im Katastrophenschutz



# Beispiel: WEGIS





# Geodatenanbieter und/oder Anwendungen in der Wirtschaft

- Straßenkarten
- Fernerkundungsdaten (Orthophotos, Satellitendaten)
- Navigation
- Ackerbewirtschaftung
- Geomarketing
- Immobilienbewertung, -vermittlung
- Standortplanung
- Location Based Services



# Geodatenzugang (1)

Wie erhält wer welche Geodaten wo?

Wie?	Wer?	Was?	Wo?
<ul style="list-style-type: none"><li>• Einsichtnahme</li><li>• Bestellung (persönlich, Brief, Fax, Internet)</li><li>• Abruf (Internet, DFÜ)</li><li>• Regelmäßige Datenübermittlung</li></ul>	<ul style="list-style-type: none"><li>• Privatpersonen</li><li>• Juristische Personen</li><li>• Öffentliche Stellen</li></ul>	<ul style="list-style-type: none"><li>• Geobasisdaten</li><li>• Geofachdaten</li><li>• Analoge Daten<ul style="list-style-type: none"><li>- Karten</li><li>- Tabellen</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Kommunen</li><li>• Landesbehörden</li><li>• Bundesbehörden</li><li>• Unternehmen</li><li>• Forschungseinrichtungen</li></ul>

# Geodatenzugang (Nutzungsbedingungen öffentliche Verwaltung)

- viele Regelungen zur Nutzung und Weitergabe von Daten:
  - Verwendungsvorbehalt, Datenschutz, urheberrechtliche Einschränkungen
- Harmonisierungsbedarf der Entgeltregelungen
- Richtlinie über Entgelte für die Abgabe und Nutzung von Geobasisdaten der Landesvermessung

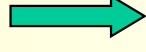
# Geodatenzugang (3)

Woher weiß man, wo man was findet und zu welchen Bedingungen?



Metainformationssysteme/Portale

- GeoMIS.Bund – Metainformationssystem für Geodaten des Bundes
- GeoPortal.Bund – Geoportal des Bundes
- Brandenburg: UDK,  
Portale der LGB und des LGRB



# Was behindert den GI-Zugang?

- Viele Datenbestände sind noch unzureichend hinsichtlich Verfügbarkeit, Aktualität, Einheitlichkeit, Flächendeckung
- Die Vertriebsstrukturen sind nicht durchgängig und es mangelt an der Transparenz der Datenangebote
- Die Preise und Nutzungsrechte an den Daten sind oft nicht marktgerecht, außerdem uneinheitlich und restriktiv
- Software für Geoinformationssysteme ist teilweise noch zu teuer und in der Bedienung nicht nutzerfreundlich

# Verbesserung des GI-Zugangs beim Bund (1)

17. Juni 1998

Kabinettschluss der Bundesregierung zur  
Koordinierung des Geoinformationswesens

8. Sep. 1998

Einrichtung des Interministeriellen Ausschusses  
für Geoinformationswesen (IMAGI) beim BMI

15. Feb. 2001

Entschließung des Deutschen Bundestages:  
Nutzung von Geoinformationen in der BRD

10. April 2003

Entschließung des Deutschen Bundestages:  
Nutzung von GI in Deutschland voranbringen

# Verbesserung des GI-Zugangs beim Bund (2)

## Bereits erreichte Ziele des IMAGI :

- Konzeption der Geodateninfrastruktur für Deutschland (GDI-DE)
- Umsetzungsstrategie beschlossen
- Pilotprojekte GDI-DE begonnen
- Transparenz der Geodatenbestände des Bundes
- Entgeltregelung des Bundes vereinheitlicht
- Zentrale Abgabe von Geodaten verbessert

# Verbesserung des GI-Zugangs (3)

## **Noch ausstehende Aufgaben in Bund und Ländern:**

- deutliche Verbesserung der Koordinierung des Geoinformationswesens in Deutschland (bund/länderübergreifend)
- Einbeziehung der Wirtschaft

## **Weg Brandenburgs:**

- Kabinettvorlage Geodateninfrastruktur Brandenburg (GIB)
- GIB-Arbeitskreis
- Zusammenarbeit mit GEOkomm

# Verbesserung des GI-Zugangs (4)

## Faktoren für die Geodatenvermarktung:

- Quantität und Qualität der Geodatenbestände
- offene und intelligente Geodateninfrastruktur
- Public Private Partnership
- einheitliche, nutzerorientierte und internetfähige Preismodelle
- flexibler und liberaler (Internet-) Zugang weitestgehend ohne Verwendungsvorbehalte zu Geodaten



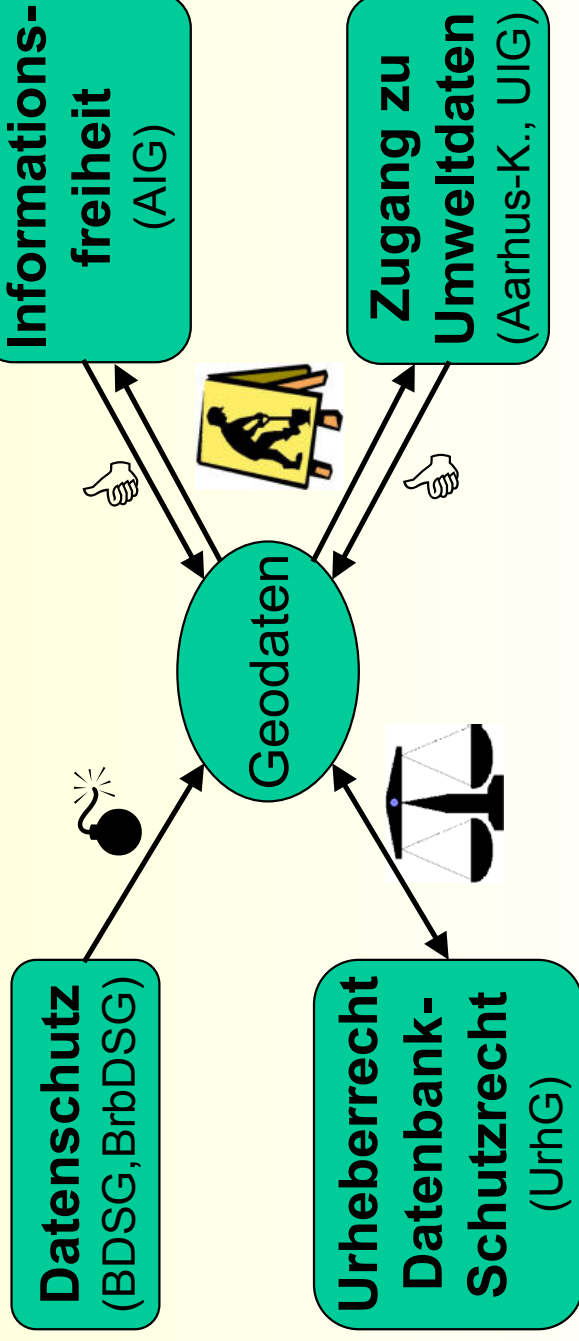
# Geoinformation im Spannungsfeld

zwischen

Restriktion

und

Forderung



# GI und Datenschutz (1)

Verallgemeinerung:

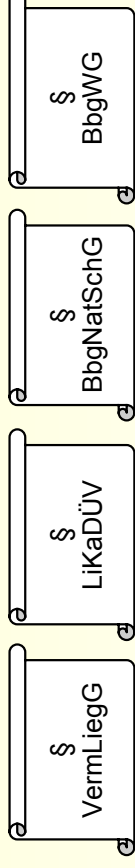
- Geodaten mit expliziten Personenangaben (Identifikation des Betroffenen möglich) unterliegen dem Datenschutz
- ohne Personenbezug sind Geodaten nicht als Personendaten zu betrachten



**Datenschutzrechtliche Fragestellungen (Rechte der Betroffenen) sind abzuwägen**

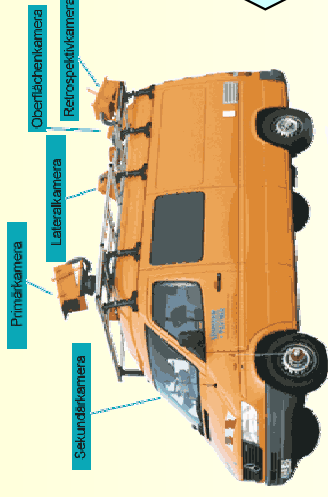
## GI und Datenschutz (2)

- Verarbeitung von Geodaten mit Personenbezug nur aufgrund gesetzlicher Normierung
  - Spezialgesetzliche Regelungen notwendig
  - Brandenburg:



- Allgemeine Regelungen für den GIS-Bereich wären Empfehlenswert (Schweizer Organisation für Geoinformation - SOGI)

# Aktuelles Beispiel



BrbDSG: ?

**Videoaufnahmen der  
öffentlichen Straßen mit  
angrenzenden Gebäuden**

**§ 9 VermLiegG:**

**Nachweis der Liegen-  
schaften (Flurstücke  
und Gebäude)  
(Lage, Nutzungsart,  
Größe, charakteris-  
tische topographische  
Merkmale)**

# GI und Urheberrechtsgesetz

- 1. Teil: Das Urheberrecht an der persönlichen geistigen Schöpfung kann bei GI am Werk selbst vorkommen (§ 2 Nr. 7 UrhG)  
Beispiel: topographische Karte, thematische Karte oder aufgrund der Auswahl und Anordnung der Elemente (§ 4 UrhG) der Datenbank
- 2. Teil, 6. Abschnitt des UrhG: Schutz des Datenbankherstellers  
§ 87 b (1): Der Datenbankhersteller hat das ausschließliche Recht, die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben.

# GI und Informationsfreiheit

## Informationsfreiheit allgemein:

- Entwurf eines Informationsfreiheitsgesetzes (Bund), Informationsfreiheitsgesetz Nordrhein-Westfalen, Schleswig-Holstein, Berlin, Akteneinsichts- und Informationszugangsgesetz des Landes Brandenburg

## Zugang zu Umweltdaten:

- Umweltinformationsgesetz
- Aarhus-Konvention

# Vielen Dank für Ihre Aufmerksamkeit !



*Institute of Applied Computer Science  
University of Linz, Austria*

---

# **The International Dimension of eGovernment: The EU Como Case Study**

**Roland Traummüller**

[traumm@ifs.uni-linz.ac.at](mailto:traumm@ifs.uni-linz.ac.at)





## eGovernment 2003 Awards

---

- 29 Countries participated with eligible countries: EU, Candidate and EFTA countries (32 in total)
- 357 cases of good praxis submitted; a 27% Increase on the respective 2001 exercise
- The study was directed by Christine Leitner (EIPA): so for more detailed information see EIPA website <http://www.eipa.nl> and [www.e-europeawards.org](http://www.e-europeawards.org)
- Three awards given (A, D, ES); 70 projects exhibited
- Report was presented at Como in July 2003 in two parts:
  - I. Statistics and analyses of good practice**
  - II. A programmatic part drawing conclusions**



## Part I: Statistics and Analyses

---

- Three general themes for submission:
  - a) A better life for European Citizens (52 %)
  - b) The role of eGovernment in competitiveness (20 %)
  - c) European, central and local government cooperation (28%)



# Statistics and Analyses: Main Trends

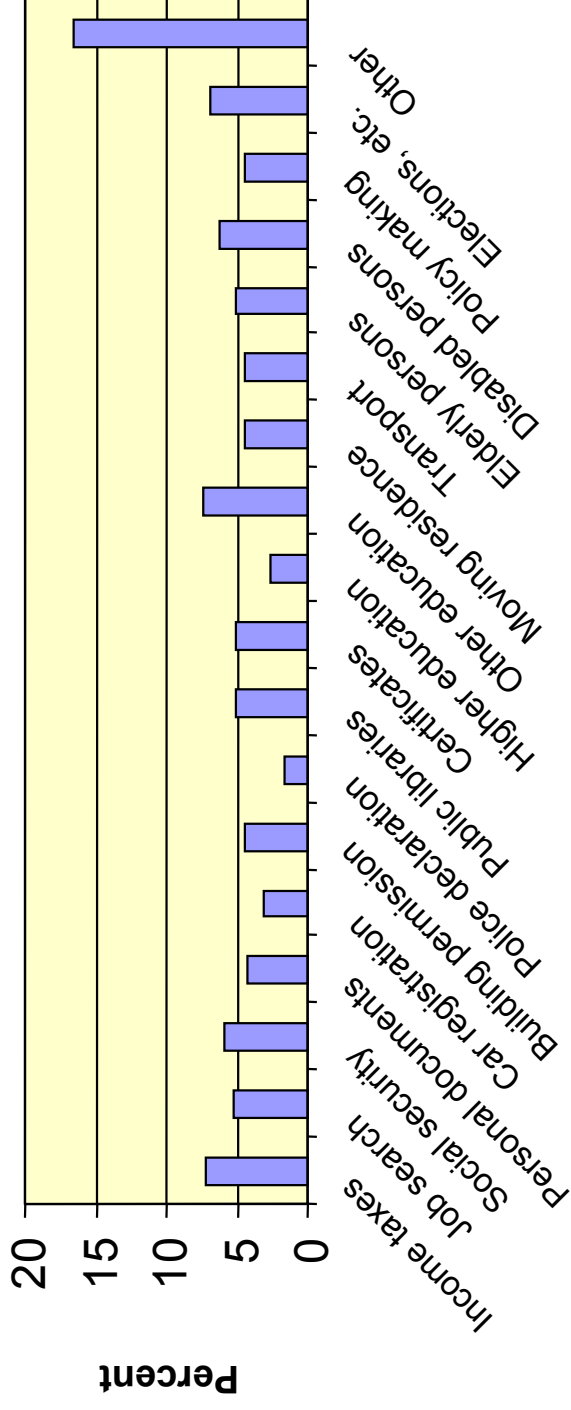
---

- Projects reveal vast differences in government competencies, population trends and cultures
- Differentiated and often highly individual solutions
- Increasing collaboration between the interest groups, private sector and government plus among administrations
- A pan-European trend in redesign of governmental processes and cutting through red tape and bureaucracy



## Results: Public eServices for citizens

as a % of all indicated under this heading in the submission form

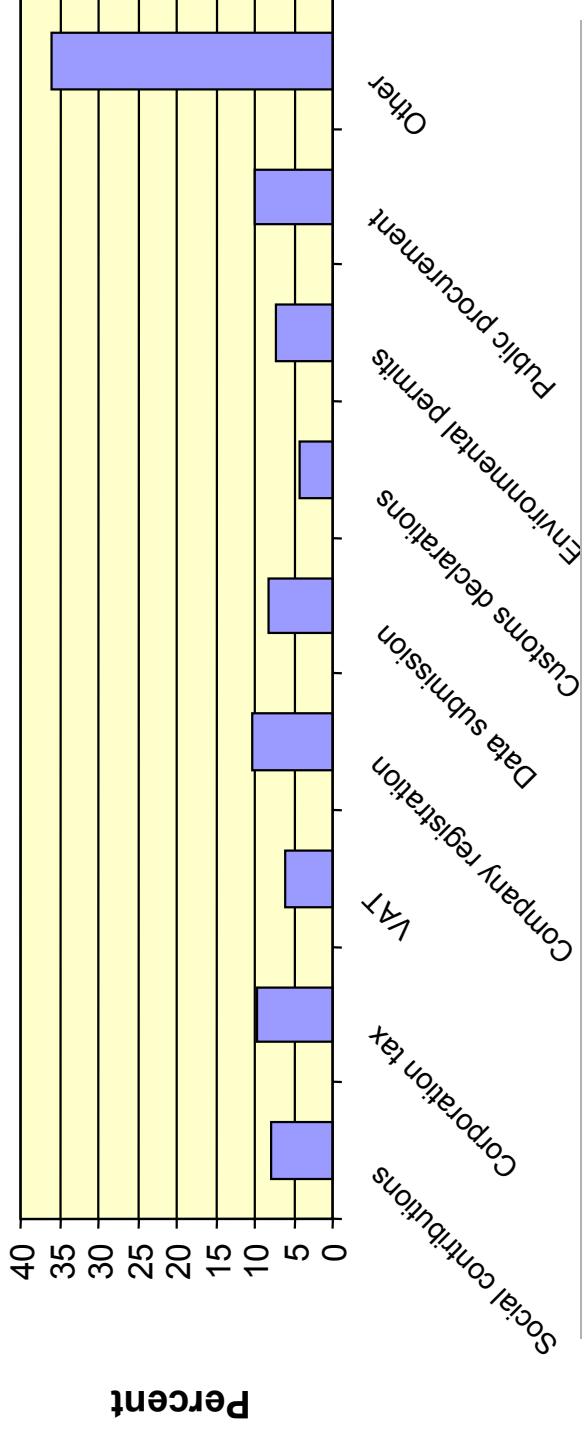


1. Education, 2. Income tax, 3. eDemocracy



## Results: Public eServices for businesses

as a % of all indicated under this heading in the submission form

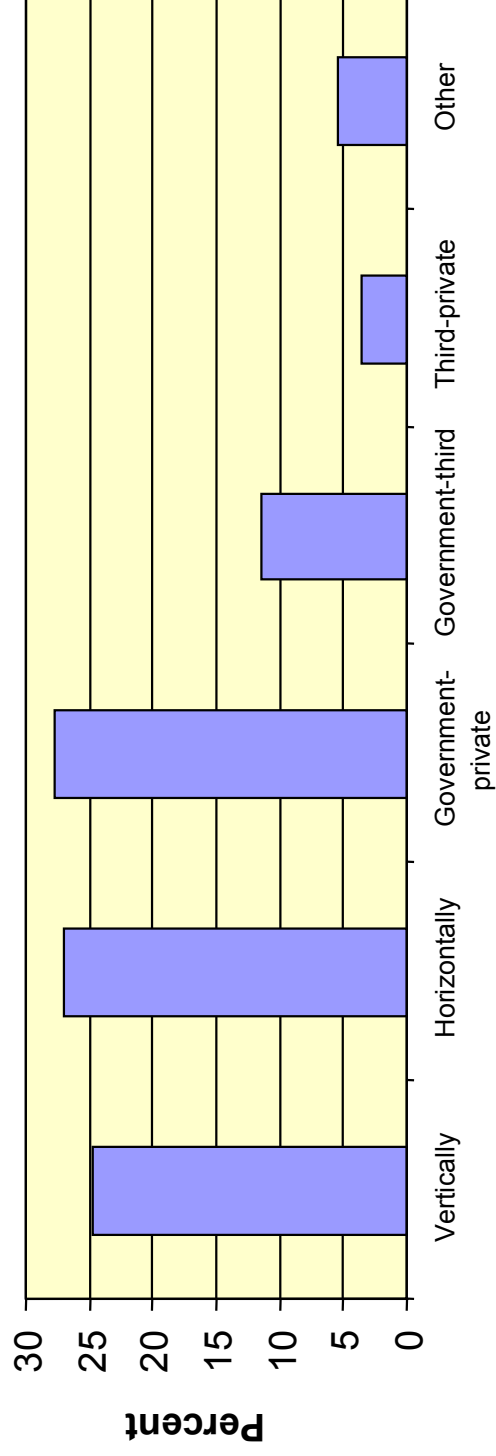


1.Registration of companies, 2.Corporation tax,  
3. Public procurement



## Results: Types of integration, cooperation and partnership

as a % of all indicated under this heading in the submission form

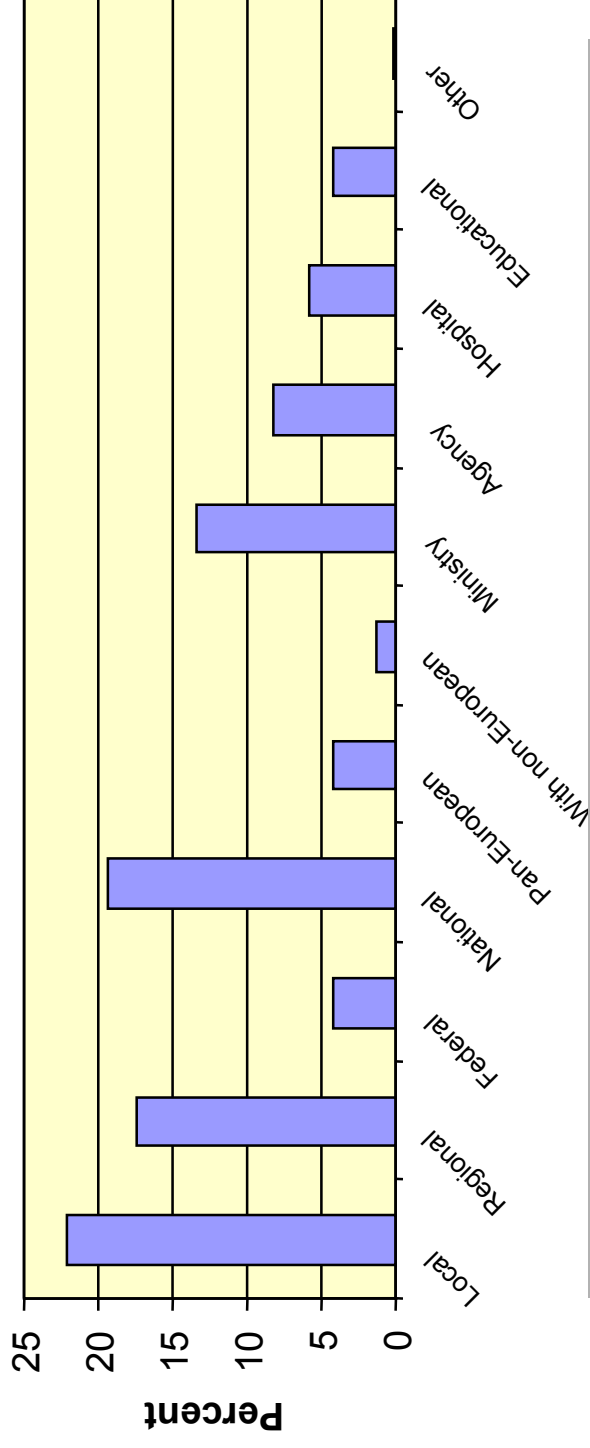


1. Government-private, 2. Horizontal, 3. Vertical



## Results: Types of levels of government organisations

as a % of all indicated under this heading in the submission form



1. Local, 2. National, 3. Regional



## Part II: A Programmatic Part

---

- Editor: Christine Leitner
- Authors: Jean-Michel Eymeri, Klaus Lenk, Morten Meyerhoff Nielsen, Roland Traummüller
- Acting as a guiding vision for modernisation
- Spurring change in giving guidance for strategies, design, implementation and change management
- The programmatic part has 30 pages in the report





## Main Features of eGovernment

---

- Four postulates are stated in Como first:
  - (1) eGovernment is the key to good governance in the information society
  - (2) eGovernment is impossible without having a vision
  - (3) eGovernment is not just about technology but a change in culture
  - (4) eGovernment is not just about service delivery but a way of life



cntd.

---

- eGovernment surpasses the administrative reform policies inspired by New Public Management (NPM)
- However, eGovernment goes further than earlier approaches to modernisation.
- It aims at fundamentally transforming the production processes of public services (not only managing them as in NPM)
- eGovernment thereby transforms the entire range of relationships of public bodies [G2C, G2B and G2G]



# eGovernance as Goal

---

- With IT governments are able to improve the quality and the accessibility of the services they offer to their citizens
- eGovernment is the key to good governance in the information society
- The outcome will be favourable and bear the marks of good governance such as democratisation, coherence, effectiveness, transparency and accountability.
- Building up a modern governance with such directions as citizen-centred, cooperative, seamless, polycentric.
- Good Governance is the goal, eGovernment is the way



# Portals Open the Way to Service Provision

---

- The prime concern; yet only the tip of the iceberg
- Regarding from two sides (client and service provider)
- Different stages of service provision: information, intention, contracting, settlement, aftercare
- **Low take-up is found and meagre usability is the reason**
- In Europe broad initiatives: post offices in France, parish churches in Portugal, tobacco shops in Austria
- Yet: One has to enable multi channel access – also in traditional ways



# Redefining Governmental Processes

---

- Mapping external service structures to internal process structures of public authorities
- Perspectives has to be complemented by a restructuring of the business processes
- Organisational front office / back office connection
- **BPR has its limitations with additional functions**
- **Protecting the rights of citizens**
- **Ensuring procedures bound to the rules of law**
- **Safeguarding privacy and legal validity**



# Categories of Processes

---

- For different ways of administrative processes the IT support will rather be different
- Recurrent and well-structured processes
- Giving advice to citizens in complex questions
- Weakly structured processes in the field of policy-making
- Processing of cases: individualised decision-making
- Negotiation processes
- Internal administrative processes



# Knowledge Enhanced Government

---

- Government has to keep up with the knowledge society
- One way is providing initiatives for promoting information society and knowledge societies
- Another way is self-reflection with administrations as intelligence organizations: officials are knowledge workers par excellence; decisions are a public official's daily bread
- So knowledge enhancement of governmental processes is a top issue
- Multiple means: knowledge repositories, software agents, avatars, invoking remote experts via multimedia
- Ultimately human and machine expertise become totally interwoven. This is knowledge enhancement at its best



# Public Services Requirements

---

- Low take up of public e-services is a big problem.
- There is no acceptance unless services become less bureaucratic and citizens see economic/individual benefits
- The needs of specific target groups must be addressed
- Provide a multi-channel access mix
- Diversity of contact points: home and mobile, kiosk, citizen office, multifunctional service shops
- Establish a high level of service integration
- Create a single-window access for all services regardless of government level and agency
- Interweaving knowledge enhancement into service processes





## Examples: Knowledge Enhancements for Public Services

---

- Giving citizens and enterprises advance information at various stages and in various depths
- Invoking remote human experts via multimedia
- Personalised portals and avatars helping in filling in forms
- Translating the demand for a service from real life into legal and administrative jargon (e.g. by personalised scenarios)
- Matching the demand with jurisdictional structures (e.g. by domain ontologies)



# Improving Citizen Participation

---

- e-Democracy intends to improve democratic decision making by stressing citizen participation
- Information becomes available to the public. This leads to more insights into how government works
- So democratic processes improving the interaction between individuals and organizations are evolving with electronic services
- Social inclusion is a problem: Special promotions for social inclusion: rural and traditionally underserved communities, the younger, the disabled



# Privacy and Security

---

- There is a general call for providing adequate level of security. An e-identity is needed in nearly all administrative transactions
- So Identity Management is a must on the basis of electronic user identification through secure authentication
- Differences between private and public sector occur at the higher level (wrong passports vs. bouncing cheques)
- The integration of back offices requires a satisfactory level of protection of personal privacy
- eGovernment across all levels including the pan-European level, brings new issues in the cross-border dataflow