

Mag. Dr. Michael Sonntag, Dr. Maria Wimmer
Johannes Kepler Universität Linz

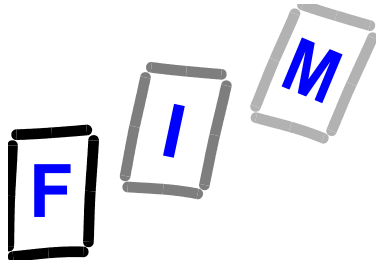
Datenschutz- und verwandte Aspekte von e-Government

Mit besonderem Bezug auf das eGOV-Projekt

Informatik 2002, Dortmund, 30.9.-3.10.2002

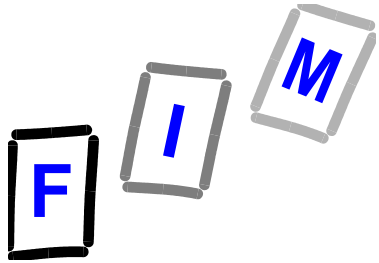
E-Mail: sonntag@fim.uni-linz.ac.at, mw@ifs.uni-linz.ac.at

WWW: <http://www.fim.uni-linz.ac.at/staff/sonntag.htm>, <http://falcon.ifs.uni-linz.ac.at/staff/maria.html>



Übersicht

- **Motivation: Das eGOV Projekt**
- **Föderalismus und One-Stop-Portale**
- **Datenaustausch zwischen Behörden**
- **Automatisierte Entscheidungen**
- **Doubletten und Bürgerkennzahl**
- **Datenschutz und Bezahlung**
- **Zusammenfassung**



Motivation: Das eGOV Projekt

EU gefördertes Projekt zur Entwicklung einer integrierten Plattform für online one-stop Government

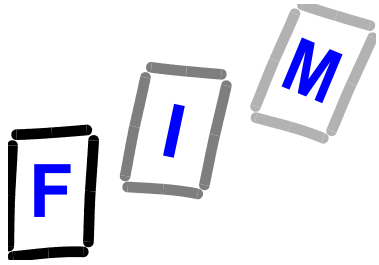
- **Partner:**

- » **Deutschland, Finnland, Griechenland, Österreich, Schweiz**
- » **Öffentl. Verwaltung, Forschungsinst., private Serviceprovider**

- **Allgemeiner (B2A, C2A) Eintrittspunkt zu allen el. Informationen unter Integration von Transaktionen**

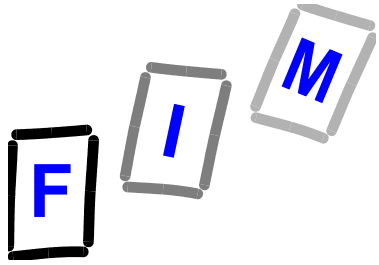
- **Einheitliches Portal + Personalisierung = Große Menge personenbezogener Daten**

→ Datenschutz besonders wichtig!



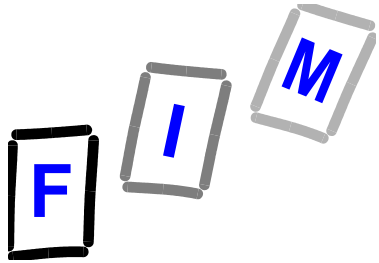
Föderalismus und One-Stop-Portale (1)

- **Föderalismus (grobe Definition; nur hier) =**
 - Verschiedene Einheiten
 - » **Bund/Länder/Gemeinden/Autonome Einheiten (z. B. Kammern)**
 - Ev. verschiedene Verfahrensvorschriften
 - Keine Über-/Unterordnung UND kein gem. Vorgesetzter
- **One stop-Portal =**
 - Einfach für Bürger: Integration / Verbergen von Details / Zentrale Anlaufstelle für alle Anliegen / ...
 - Zentral: Management / Administration / Backups / ...
 - Daten von vielen Einheiten verwendet (auch für Teile anderer Einheiten!)



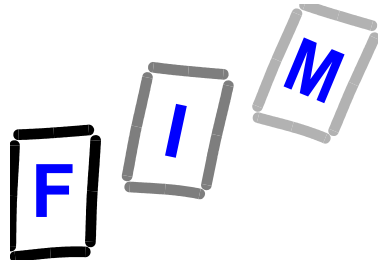
Föderalismus und One-Stop-Portale (2)

- **Zwei Rollen: Datenverarbeiter \Leftrightarrow Dienstleister**
 - Portalbetreiber- Eigene Verfahren: Kein Problem
 - Portalbetreiber - Verfahren anderer Einheiten
 - » **Dienstleister: Vereinbarung über jede Verarbeitung erforderlich**
 - » **Datenzugriff: Wie, Wann, Wofür?**
- **Beispiel: Formulare mit ext. Daten vorausfüllen**
 - Bürger fragt nach eigenen Daten und transferiert sie zu einer anderen Einheit
 - Portal ist hier Dienstleister für den Bürger
- **ANDERS: Portal verwendet Daten zur Entscheidung bei Personalisierung!**



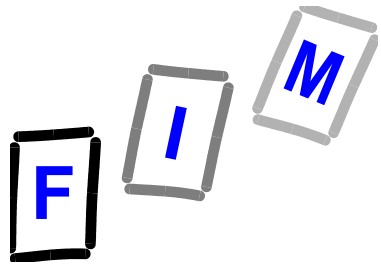
Amtshilfe zwischen Behörden

- **Meist keine Gefahr für den Datenschutz**
 - Formelles Verfahren
 - Schriftlich: Jede Anfrage hinterläßt Spuren
 - Individuelle Begründung erforderlich
 - » „Offizielle“: Für eine Entscheidung oder anderen „Inhalt“ benötigt
 - Überprüfung, ob diese Information weitergegeben werden darf
- **One-stop Portale:**
 - Kein formelles Verfahren: Automatische Durchführung
 - Nur generelle Begründungen: „In solchen Fällen erlaubt“
 - » Nur typische Fälle; individuelle Umstände werden NICHT geprüft!
 - Auch für andere („nicht-offizielle“) Zwecke verwendet:
 - » Personalisierung, Hinweise, Vor-ausfüllen von Formularen, ...



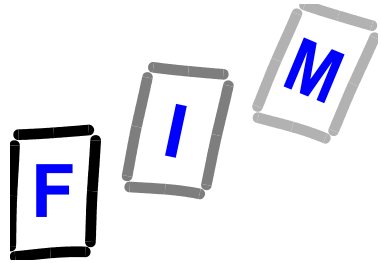
Datenaustausch zwischen Behörden (1)

- **Falls Austausch erlaubt; wie wird er durchgeführt?**
 - ➔ **Überprüfung: Wer verlangt welche Daten wofür?**
 - » **Definition nötig: Welche Daten & welche Gründe; wer darf bestimmt begründete Anforderungen abschicken**
 - ➔ **Versand: Daten müssen maskiert werden**
 - » **Nur die benötigten Daten dürfen gesendet werden, nicht alles**
 - » **Daher riesige Menge an unterschiedlichen Datendefinitionen**
 - » **Identifikation der Datendefinition pro Transaktion erforderlich**
 - » **Verschlüsselung, Identifikation des Empfangsservers, ...**
 - ➔ **Speicherung: An einen bestimmten Zweck gebunden**
 - » **Dürfen nur für den vereinbarten Zweck gespeichert werden**
 - » **Problem: Personalisierung = Verbindung mit anderen Daten**



Datenaustausch zwischen Behörden (2)

- **Wahrscheinlich beste Lösung: XML-basierend**
 - Besser große Lösung: Keine Begrenzung auf Teilbereich
- **Organization ebenso wichtig**
 - Wie werden Anfragen erstellt / abgeschickt
 - Benutzeridentifikation / Logging
 - Kopien oder externe Referenzen?
- **Prozess-Änderung ebenfalls wichtig**
 - Schnittstellen in el. Aktenverarbeitungssystemen
 - Ablösung alter und definition neuer Anfragen / Antworten
 - Für Datenschutz verantwortliche Person
 - **Mitarbeiterausbildung**



Datenaustausch zwischen Behörden (3)

- **Referenzen oder Kopien?**

- **Technisch: Referenzen komplex, Kopie einfach**

- **Rechtlich: Referenzen aufwendig, Kopie einfach**

- **Datenschutz: Kopie eher vorzuziehen!**

- » **Nur einmalige Übertragung erforderlich**

- » **Übermittlung erfolgt an Betroffenen selbst ⇒ meist kein Problem**

- » **Keine zeitliche Abfrage nötig: Daten bleiben konstant**

- » **Inkonsistenzen können entstehen: Erschweren Datenabgleich**

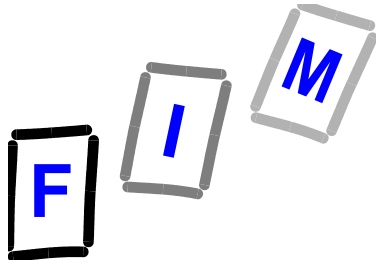
- **Vorteile von Referenzen**

- » **Keine Mehrfachspeicherung (Gefahr der Weitergabe)**

- » **Immer aktuelle/korrekte Daten**

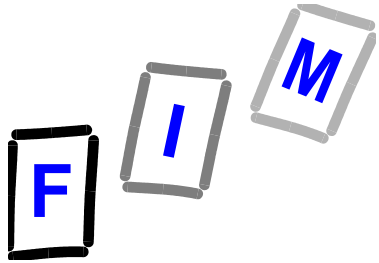
- » **Leichtere Zugriffssicherung**

- » **Daten unter Kontrolle der zuständigen & verantwortlichen Stelle**



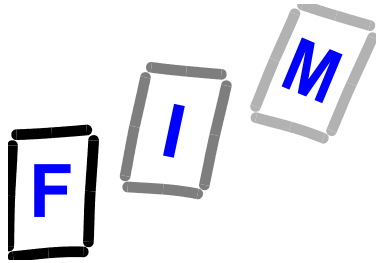
Automatisierte Entscheidungen (1)

- **Einfaches Verfahren & alle Unterlagen online**
 - » (El. signierte oder aus sicheren Datenbanken) Dokumente, andere Datenbanken, öff. Verzeichnisse...
 - Automatisierte Entscheidung möglich
 - » Beispiele: Hundesteuer, Verlängerungen, Beantragung von Urkunden, Wohnsitzmeldung, etc.
- **Probleme:**
 - Identifikation des Bürgers
 - El. Sammlung der Unterlagen erforderlich
 - Bezahlung sollte geschützt/anonym sein
 - Bescheide ohne menschliche Mitwirkung möglich?
 - Länder-Verfahren durch Bund/Private durchgeführt?



Automatisierte Entscheidungen (2)

- **Ist eine Unterschrift erforderlich?**
 - » **Rechtlich bindende Signaturen sind automatisch nicht möglich!**
- **Menschliche Entscheidung erforderlich?**
 - » **Reicht die Entscheidung zum Einsatz eines Programmes aus?**
- **Kann jemand Bescheide für Andere “erzeugen”?**
 - Meist kein Problem, die Inhaltsentscheidung muß jedoch bei der “eigentlichen” Einheit verbleiben!
- **Wie rasch kann das Programm verändert werden?**
 - Muß sofort möglich sein (zumindest Abschaltung)
- **Was passiert mit den verwendeten Daten?**
 - Speicherung im Portal, zur Behörde transferiert, ...?



Doubletten

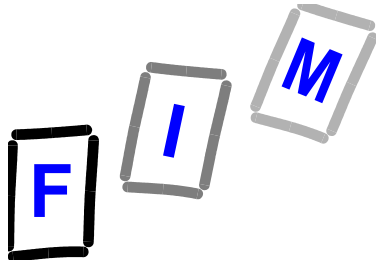
1 Person - 2 Datensätze

- **Gründe:**

- Schreibvarianten: Müller - Mueller - Muller
- Vergessene (Kunden-)nummer
- Fehler, Backups, kurzzeitige Ausfälle: Besser doppelt als gar nicht

- **Konsequenzen:**

- Probleme mit Personalisierung
- Ergebnisse/Entscheidungen nicht vorhersehbar
- Auskunftsrecht gefährdet
- Updates führen zu inkorrekten Daten (im anderen Satz)



Doubletten

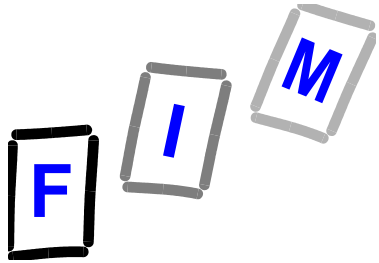
2 Personen - 1 Datensatz

- **Gründe:**

- Ähnliche Namen: Besonders ausländische Schriften (z.B. arabisch, kyrillisch, ...)
- Zu wenige Identifikationsdaten: Name und Geburtsdatum reichen nicht aus
- Vertretung: “Mach’s schnell für mich”

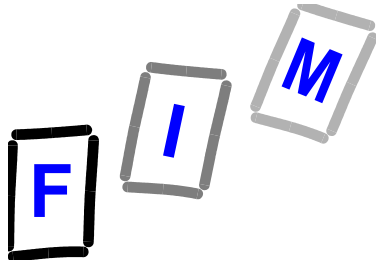
- **Konsequenzen:**

- Probleme mit Personalisierung
- Ergebnisse/Entscheidungen nicht vorhersehbar
- Recht auf Korrektur gefährdet
- Eine Person geht bei Korrektur “verloren”
- Daten von einer Person werden der anderen mitgeteilt



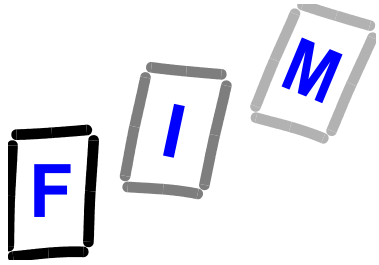
Eindeutige Bürger-Kennzahl

- **Nicht wirklich eine Lösung:**
 - Ohne Nummer geht gar nichts!
 - » **Oder Suche nach ihr mittels andere Daten ⇒ Gefahr von Doubletten!**
 - Jede einzelne Datenbank müßte geändert werden
 - Kosten für die Verteilung der Nummern
 - Überprüfung, daß eine Person zu einem Nummer gehört
 - Person = Nummer ???
- **Gute Idee für:**
 - In jeder Datenbank eine eigene eindeutige Nummer
 - Als zusätzliche (freiwillige) Möglichkeit
 - Vermeidung von Datenschutzproblemen durch Maskierung (siehe z. B. ZMR in Österreich!)



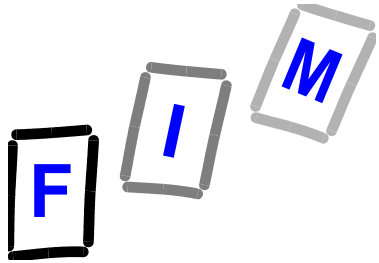
Datenschutz und Bezahlung (1)

- **Früher: Bargeld/Stempelmarken: Anonym**
- **Heute: Elektronischer Transfer**
 - ➔ **Vollständig individualisiert**
 - » **Kontobesitzer, Kreditkartennr., autorisierende Person, Bonität,...**
 - ➔ **Alles muß für spätere Überprüfungen gespeichert werden**
 - ➔ **Gefahr besonders bei Kombination mit anderen Daten**
- **Voraussetzung für el. Verfahren:**
 - ➔ **Verfahrensbindung, Betrag und Währung, Datum, Empfänger**
 - ➔ **El. Validierung muß möglich sein (am besten sofort)**
 - » **Sollte kein Beweis für Auftrag sondern Durchführung sein!**



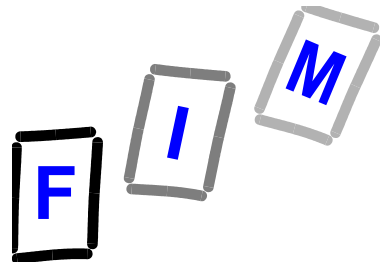
Datenschutz und Bezahlung (2)

- **Bezahlung sollte unabhängig vom Portal sein**
 - » **Verschiedenste Zahlungsmöglichkeiten akzeptieren**
 - » **Kein neues Zahlungssystem, sondern existierende einbinden**
- **Vorteil: Teilnehmer sind ohnehin sicher identifiziert!**
- **(Teilweise) Lösung: El. Zahlungsbestätigung durch Österr. Banken wird zu Jahresende verfügbar sein**
 - **Elektronisch signierter Ersatz für Überweisungsformulare**
 - **Enthält jedoch noch alle personenbezogenen Daten**
 - **(Spätere) Anonymisierung voraussichtlich nicht möglich**
- **Portal könnte als Anonymizer dienen**
 - » **Problem: Ist selbst unter staatlicher Kontrolle!**



Zusammenfassung

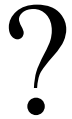
- **Integrierte one-stop Portale sind SEHR hilfreich**
 - Rechtliche Probleme: Datenschutz
 - Diese sind kompliziert und Bürgern schwer zu erklären
 - Konkludente Zustimmung verwenden wo möglich
- **Datenaustausch zwischen Behörden ist Notwendigkeit**
 - Minimalitäts-Prinzip
 - Inkonsistenz-Probleme aufgrund mehrfacher Quellen
- **Automatisierte Entscheidungen oft möglich**
 - Jedoch nur für sehr eng begrenzte Bereiche
- **Datenschutz bei el. Bezahlung wichtiger als früher**



Mag. Dr. Michael Sonntag, Dr. Maria Wimmer



Fragen?



Vielen Dank für Ihre Aufmerksamkeit!



E-Mail: sonntag@fim.uni-linz.ac.at, mw@ifs.uni-linz.ac.at

WWW: <http://www.fim.uni-linz.ac.at/staff/sonntag.htm>, <http://falcon.ifs.uni-linz.ac.at/staff/maria.html>