

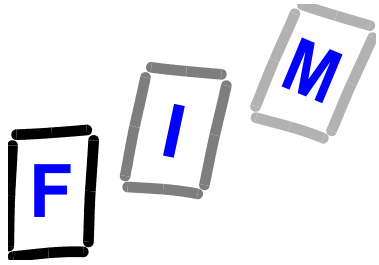
Mag. Dipl.-Ing. Dr. Michael Sonntag

Privacy issues of e-Government

Wroclaw Summer School, Wroclaw, 19.9.-21.9.2002

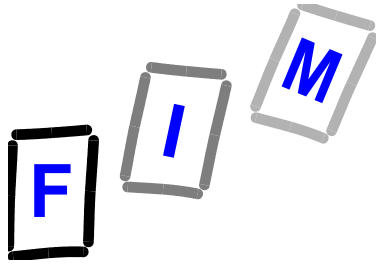
E-Mail: sonntag@fim.uni-linz.ac.at

WWW: <http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



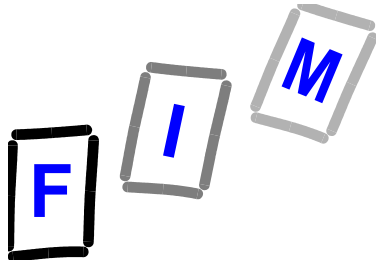
Content

- **Motivation**
- **Federalism and One-Stop-Portals**
- **Data exchange between authorities**
- **Automated decisions**
- **Identification of users**
- **Conclusions**



Motivation

- Public administration should be model of excellence
- Changing status of portals
 - Information \Rightarrow Few personal data
 - Transactions \Rightarrow Lots of personal data
- Largest advantage AND largest risks by integrating data from many sources
 - \rightarrow Different ministries, health data, tax information, ...
- Danger: **Person=Number \Rightarrow No number=No Person!**
- eGOV project



Federalism and One-Stop-Portals (1)

- **Federalism =**

- » **Loose definition; only used here**

- **Different entities**

- » **Federal / state / municipal / autonomous level**

- **Different rules of procedure (possibly)**

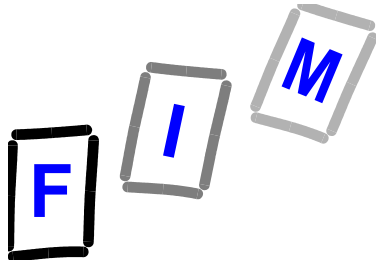
- **No super-/subordination**

- **One stop portal =**

- **Simple for citizens: Fully integrated / details hidden**

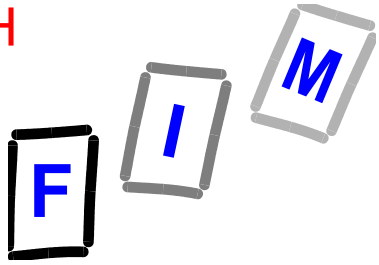
- **Centralized: management / administration / backup / ...**

- **Data from many entities used (also for parts of others!)**



Federalism and One-Stop-Portals (2)

- **Different roles: Controller \Leftrightarrow Processor**
 - Portal operator - own proceedings: No problem
 - Portal operator - proceedings of other entities
 - » Serves as a processor - Contract on each process required
 - » Data access: How, when, for what?
- **Example: Filling in forms with external data**
 - User asks for own data and transmits it to another entity
 - Portal is here processor for the user
- **DIFFERENT: Portal uses data to decide what to present the user (personalization)!**



References or copies?

- **Reference:**

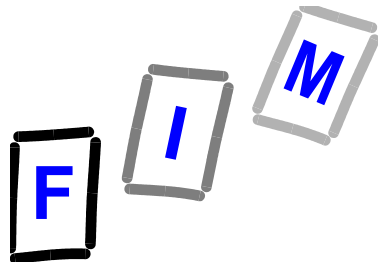
- » Transmission on every use
- » Privilege of “Processor” not applicable
- » Exemptions not applicable
- » Explicit consent of user needed
- » Always current data

→ Avoid; unless current data necessary (e. g. address)

- **Copy:**

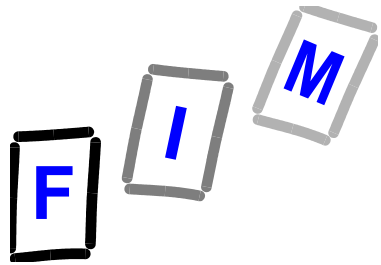
- » Transmission only once, on order by the citizen
- » Data stays as it was in the application
- » Consent can be implicit

→ Prefer; less privacy problems



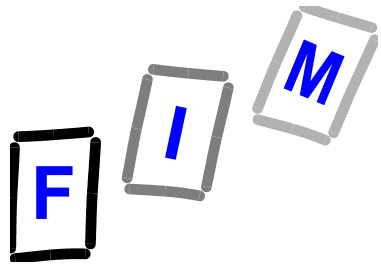
Data exchange between authorities (1)

- **If exchange is allowed, how will it be done?**
 - ➔ **Verification: Who requests, which data, for what?**
 - » **Definition required which data may be sent for which reasons, who might send requests with certain reasons**
 - ➔ **Sending: Data must be masked**
 - » **Only the authorized data may be sent, not the whole file**
 - » **Therefore huge number of different data sets**
 - » **Identification of data set per transaction, not unique**
 - » **Encryption, partner server identification, ...**
 - ➔ **Storage: Bound to single purpose**
 - » **May be stored/used only for the purpose it was acquired for**
 - » **Problem: Personalization requires relating it to other data**



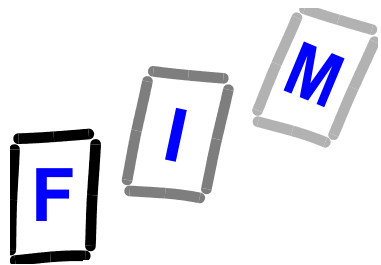
Data exchange between authorities (2)

- **Probably best solution: XML-based language**
 - Should be a large solution: Not confined to small area
- **Organizational issues also important**
 - How to place requests
 - Identification of users / Logging
- **Processes must be adapted**
 - Interfaces in electronic record handling systems
 - Retirement of old / definition of new requests / responses
 - Person responsible for privacy
 - User education



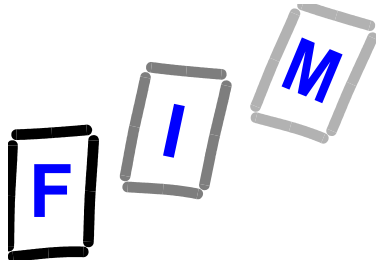
Automated decisions (1)

- **Simple procedure & everything available online**
 - » **El. signed documents, other databases, ...**
 - **Automated decisions are possible**
 - » **Examples: Dog tax, prolongations; paying adm. fines, etc.**
- **Problems:**
 - **Identification of the citizen**
 - **Gathering of evidence needed**
 - **Payment should be anonymous**
 - **Art. 15 applicable? No problem if course of law available**
 - **Notifications without humans possible?**
 - **State proceedings done by a federal system**



Automated decisions (2)

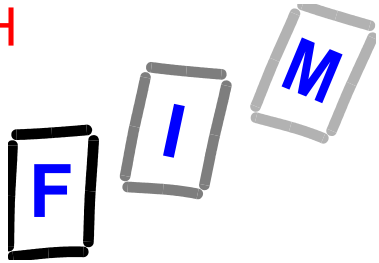
- **Must there be a signature?**
 - No autonomous (legally binding) el. signatures!
- **Is a human decision required?**
 - Or is the decision to use a certain program sufficient?
- **May an entity “produce” decisions for others?**
 - Usually no problem
 - Decision about content must remain by the authority!
- **How fast can changes be made to the program?**
 - Must be possible immediately
- **What is to be done with the data involved?**
 - Stored at the portal, moved to the authority, ...?



Identification of users

- **General issues of privacy**
 - » Cookies, passwords; users's consent; logfiles, ...
- **Using el. signatures for identification**
 - » Not a good idea, that's not what they are there for
 - » Distracts from importance of signing
- **Automatic log-out**
 - » Personalized information already sensitive
- **Must be secure and reliable**
 - » Official delivery of notifications impossible otherwise

Use (general) chipcard and keep it inserted



Doublettes

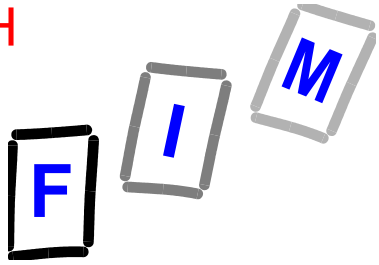
1 Person - 2 Data sets

- **Reasons:**

- Spelling variants: Müller - Mueller - Muller
- Forgotten (customer-)number
- Errors, backups, temporary failures: Better double than nothing

- **Consequences:**

- Problems with personalization
- Results/decisions unpredictable
- Right of access endangered
- Updates lead to incorrect data (in other set)



Doublettes

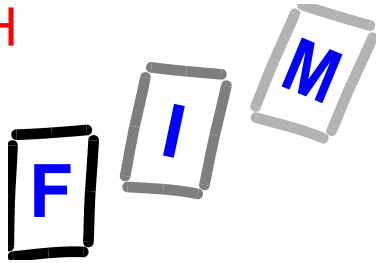
2 Persons - 1 Data set

- **Reasons:**

- Similar names: Especially if foreign script (e. g. arabic)
- Too few data for identification: Name & DoB insufficient
- Impersonation: “Just do it for me”

- **Consequences**

- Problems with personalization
- Results/decisions unpredictable
- Right of correction problematic
- One person is “lost” on correction
- Data from one is revealed to the other



Unique numbering of citizens

- **Not really a solution:**

- If number unknown, nothing is possible

- » Or searching for it using other data ⇒ danger of doublettes!

- Every database would have to be changed to it

- Costs of distributing the number

- Verifying the person matches the number

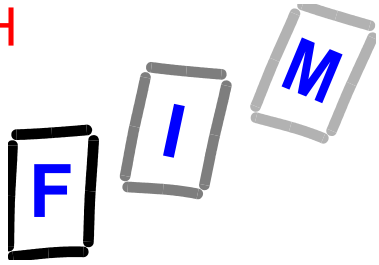
- Person = Number

- **Good idea for:**

- In each database a unique number

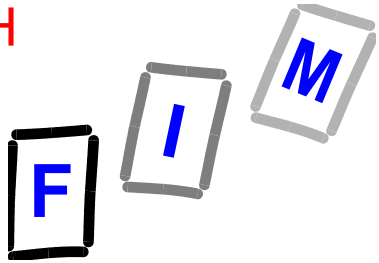
- As additional possibility (voluntary)

- Avoid privacy dangers by masquerading it (⇒ ZMR!)



Privacy issues of payment (1)

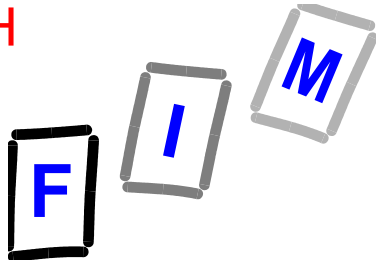
- **Past: Payment in cash / special stamps**
 - Completely anonymous
- **Now: Electronic transfer**
 - Completely individualized
 - » Owner / number of the bank account or credit card, ...
 - » Authorizing person (signature on transfer form)
 - » Credit standing (inquiry about credit cards)
 - Must all be stored for later verification
 - Danger if combined with other data
 - » Income tax might be interested!
 - **BUT: Precondition for electronic proceedings!**



Privacy issues of payment (2)

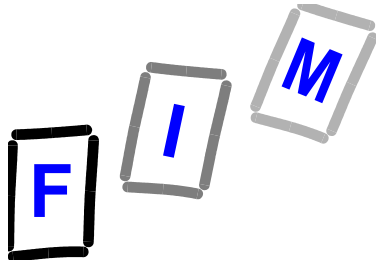
- **What's required of el. payment for proceedings:**
 - Connection to proceeding: Useable only once
 - Amount of money (+currency)
 - Date of payment: In time?
 - Recipient: Correct body (country, chamber, ...)?
 - Electronic validation possible: In best case instantly
 - » **Not proof of order but of fulfillment!**
- **Should be independent of portal**
 - » **Different solutions from any bank should be accepted**
 - » **No new payment system, use existing ones for larger audience**

Advantage: Partner VERY securely identified anyway!



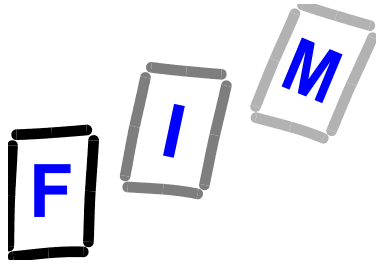
Privacy issues of payment (3)

- **(Partial) solution: Electronic payment confirmation by Austrian banks will be available end of year.**
 - ➔ Electronically signed replacement of transfer form
 - ➔ Still contains all the personal information
 - ➔ Probably no removal without invalidating the signature
 - ➔ Event then the bank is still discernible
- **Anonymizer (officially approved!) needed:**
 - ➔ Verifies information
 - ➔ Removes sensitive data
 - ➔ Appends own signature



Conclusions

- **Integrated one-stop portals are VERY helpful**
 - They pose legal problems: Privacy
 - Complicated and difficult to explain to citizens
 - Use implied consent where possible
- **Data exchange between authorities is necessary**
 - Principle of minimalism
 - Cope with inconsistencies because of multiple sources
- **Automated decisions usually possible**
 - Only for severely restricted areas
 - Depends on multiple small issues in local law



Mag. Dipl.-Ing. Dr. Michael Sonntag



Questions?



Thank you for your attention!



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

WWW: <http://www.fim.uni-linz.ac.at/staff/sonntag.htm>