Privacy from Womb to Tomb

Delegation from a European Perspective

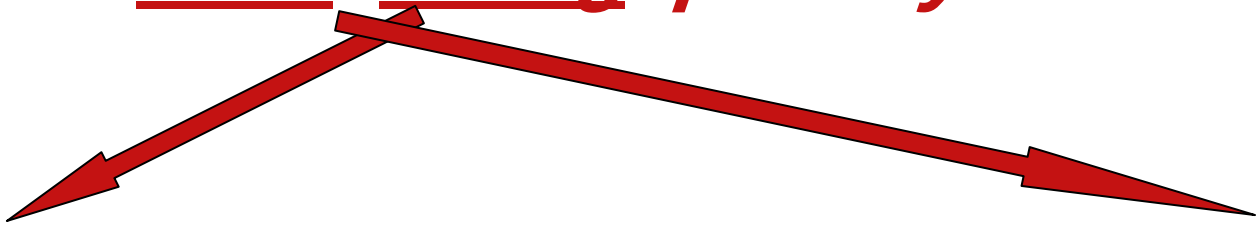
Marit Hansen, Maren Raguse, Katalin Storf,
Harald Zwingelberg

IFIP / PrimeLife Summer School
8 September, 2009 in Nice

http://www.primelife.eu/

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

life long privacy



long privacy

- linkability of partial identities
- lack of transparency
- enforcing data subjects rights
- anonymity and pseudonymity
- advance in biometric identification
- security of crypto algorithms

⇒ user control

⇒ privacy-enhancing IDM, PETs

privacy throughout life

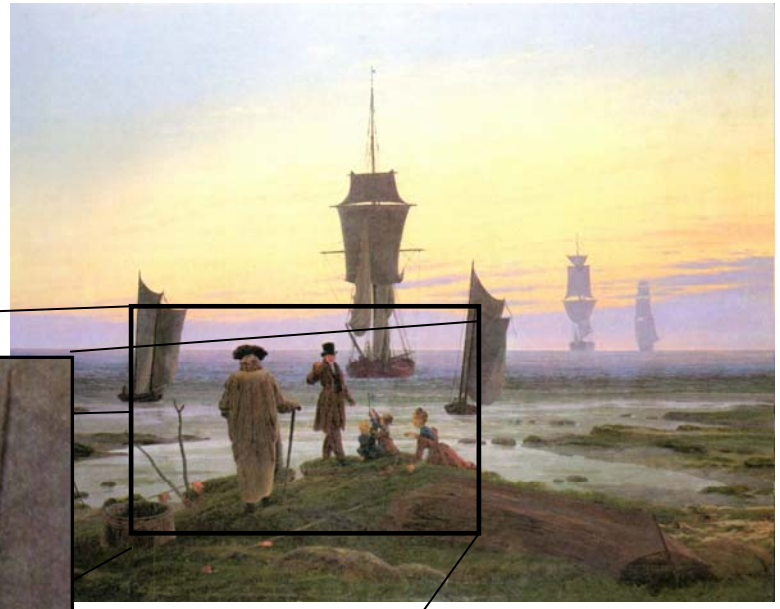
- privacy for children, elderly and disabled persons
- enforcement of data subjects rights by for incapable persons
- management of partial identities

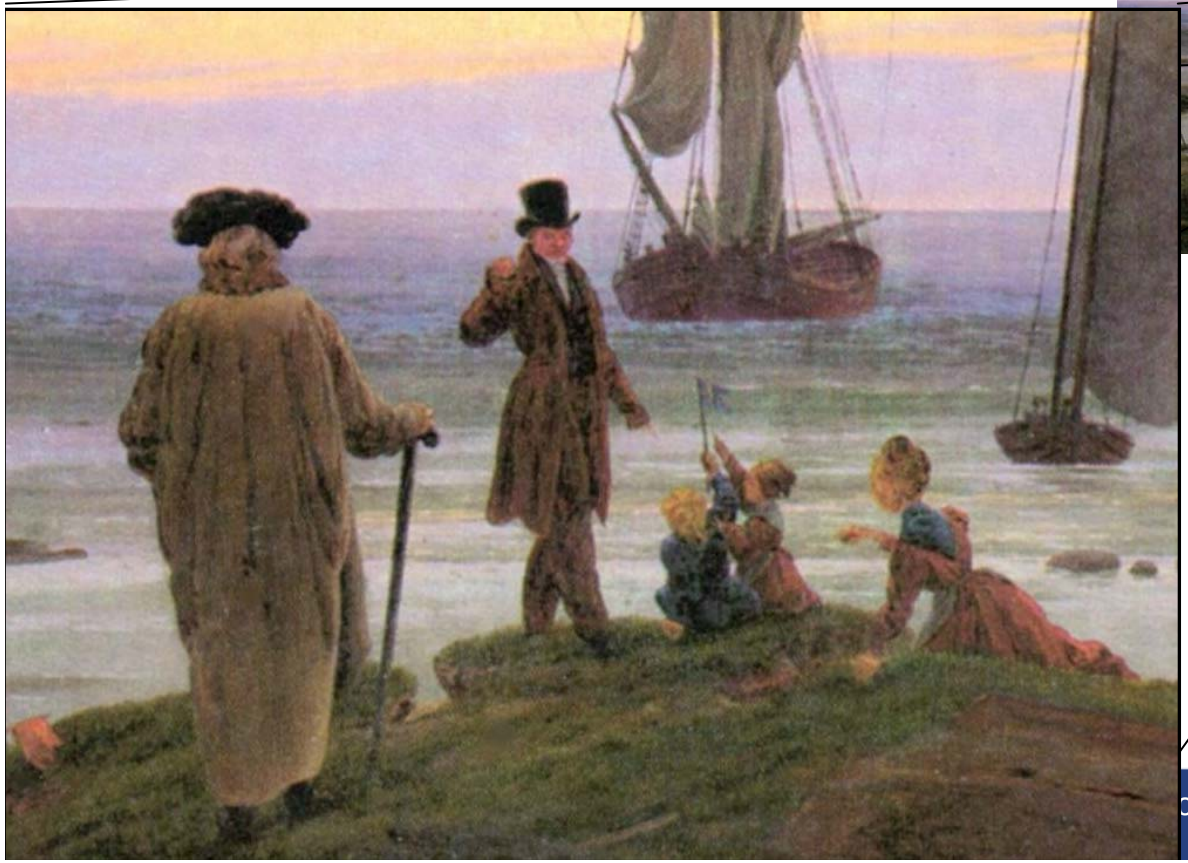
identified problem:

⇒ maintaining privacy in all stages of life

stages of life

Famous artist reflecting on
"The Stages of Life"
("Die Lebensstufen")





Caspar David Friedrich, about 1835 depicting childhood, adulthood, old age and eventually death using oil in canvas.
(picture is public domain, source wikipedia)

stages of life

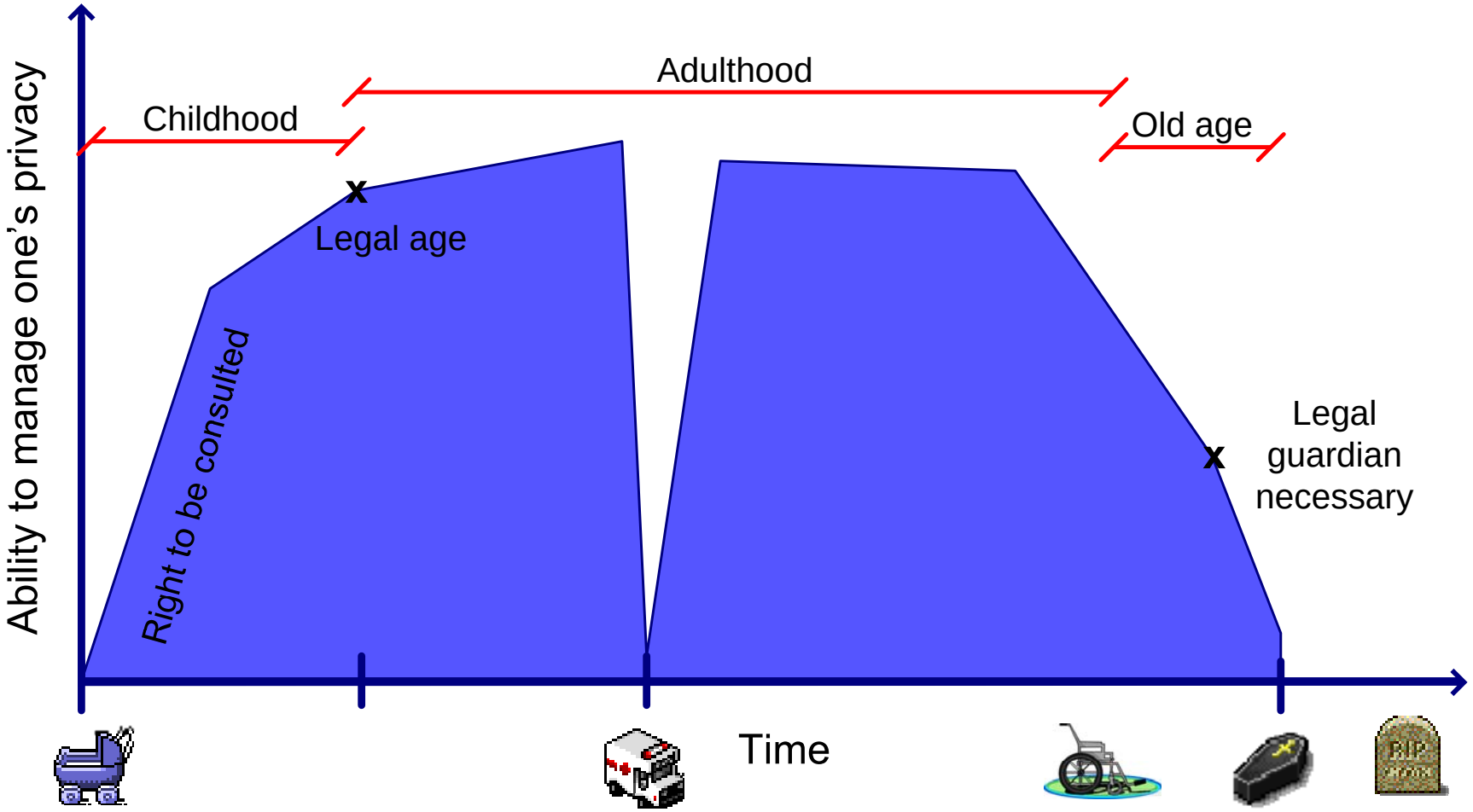
Our focus: capability to handle one's own privacy

A stage of life of an individual wrt to managing his privacy is a period of life in which his ability to do so remains between defined boundaries characterising this stage of life.

Such stages include:

- prenatal
- childhood
- adulthood
- temporary incapability
- old age
- death
- post-mortal period

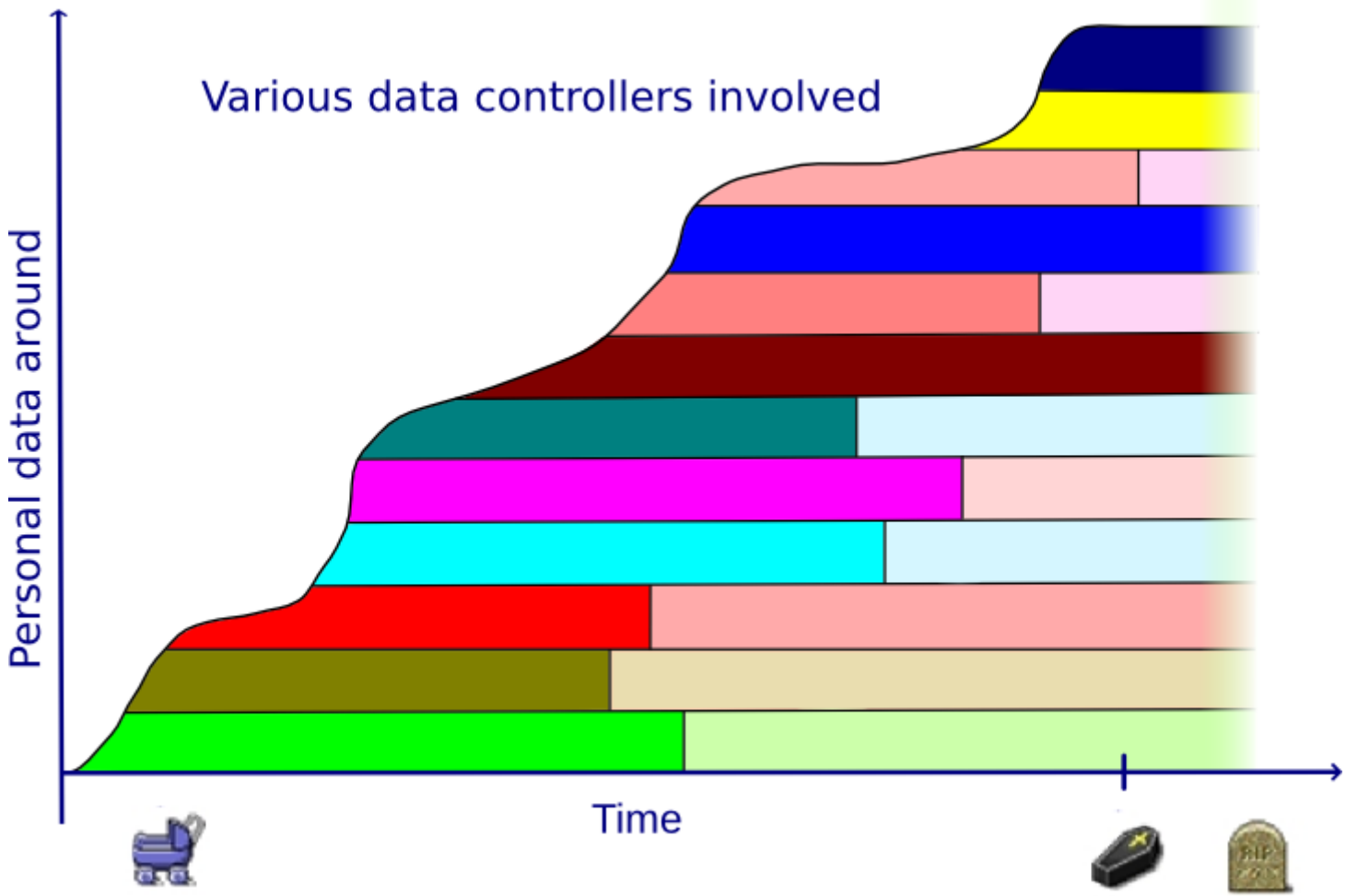
ability to manage one's privacy



solution: delegation

- delegation is an evident solution
- **delegation** is a process where a **proxy** is authorised to act on behalf of a **principal** via a mandate, i.e., by transferred rights, duties and the required authority to act
- in this talk:
  focus on **natural persons** for principal and proxy
- delegation is well known as agency [law] in the legal sphere, in particular in private law
- but these rules are not easily transferable to privacy ...

disclosure of data over lifetime



factual problems for principals

perspectives

- young adults reaching maturity
- persons that have temporarily been represented by a proxy

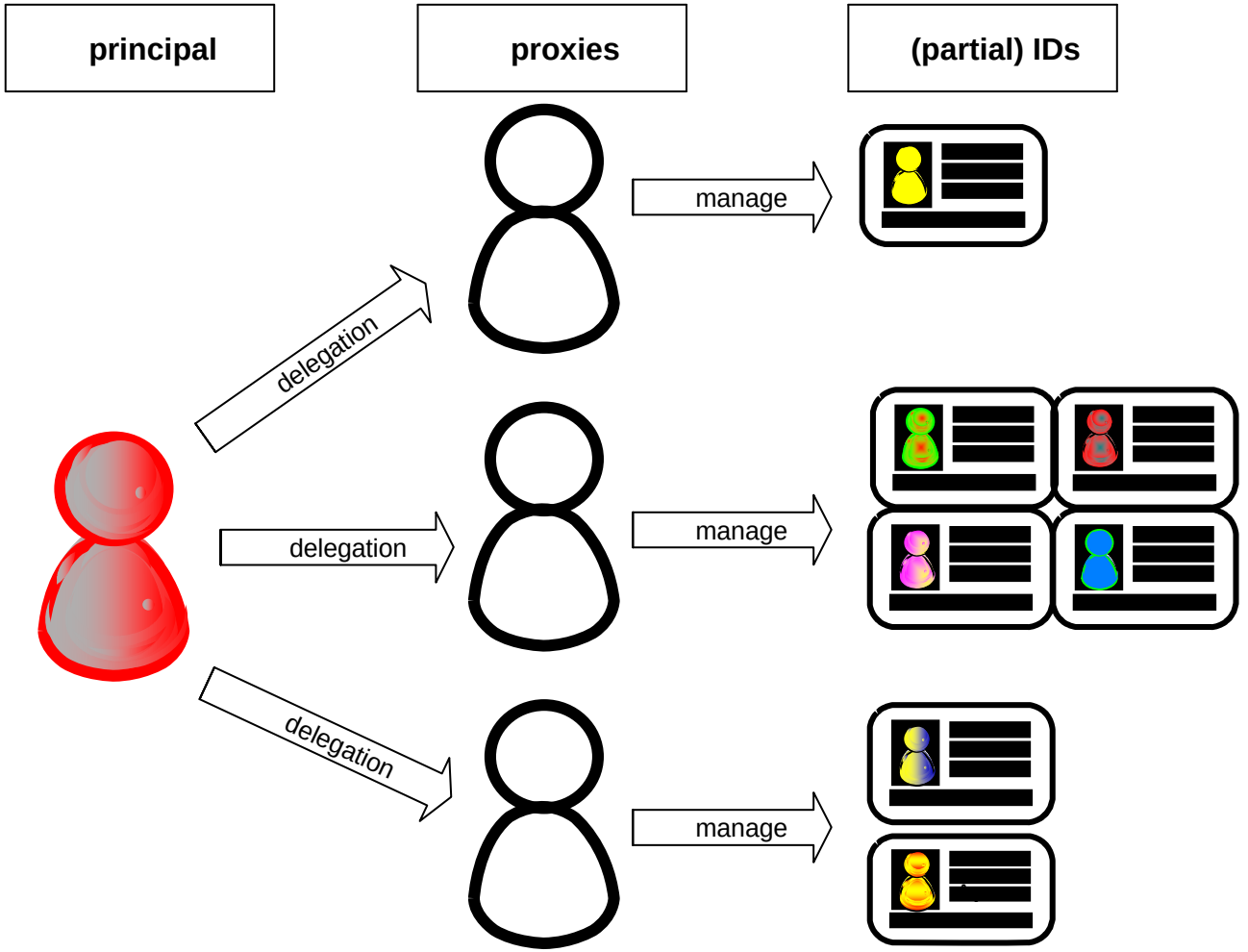
problems

- lack of traceability of former decisions concerning one's privacy
- data has been spread to others meanwhile

⇒ **solution**: data track

⇒ raising other questions

issues raised by data tracks



whose data track to use?

should proxies see / know of each other?

“master proxy”: seeing all (p)IDs?

succession of proxies?

who is data controller?

lacking support of proxies

- current applications and services (web shops etc.) do not natively support proxies (yet)
- principal is currently forced to share access credentials
- not distinguishable who actually acted

⇒ legal and technical support necessary

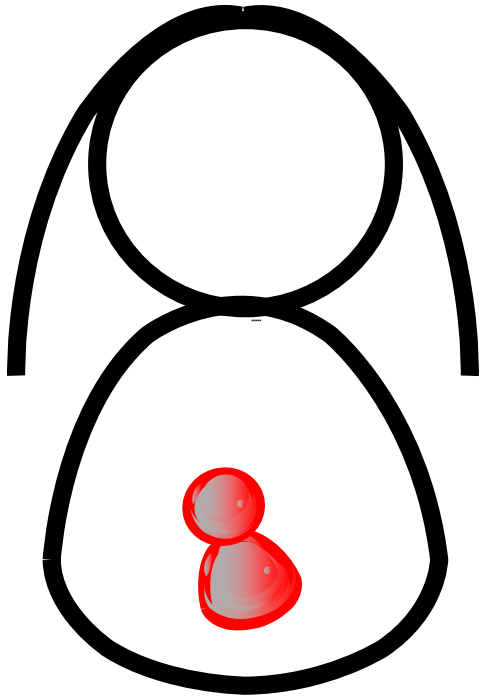
preferences ...

- principals should be enabled to define preferences, guidelines, conditions

- binding to preferences etc. must not be overstrained
  - lack of volunteers
  - often proxies are laymen
  - conflicting rules (e.g., legal custodian)
  - priority of other duties (organising homecare, ...)

- fallback option: lawmakers should define general guidelines (e.g., based on data minimisation defining proportionate exceptions)

womb: prenatal phase



challenges

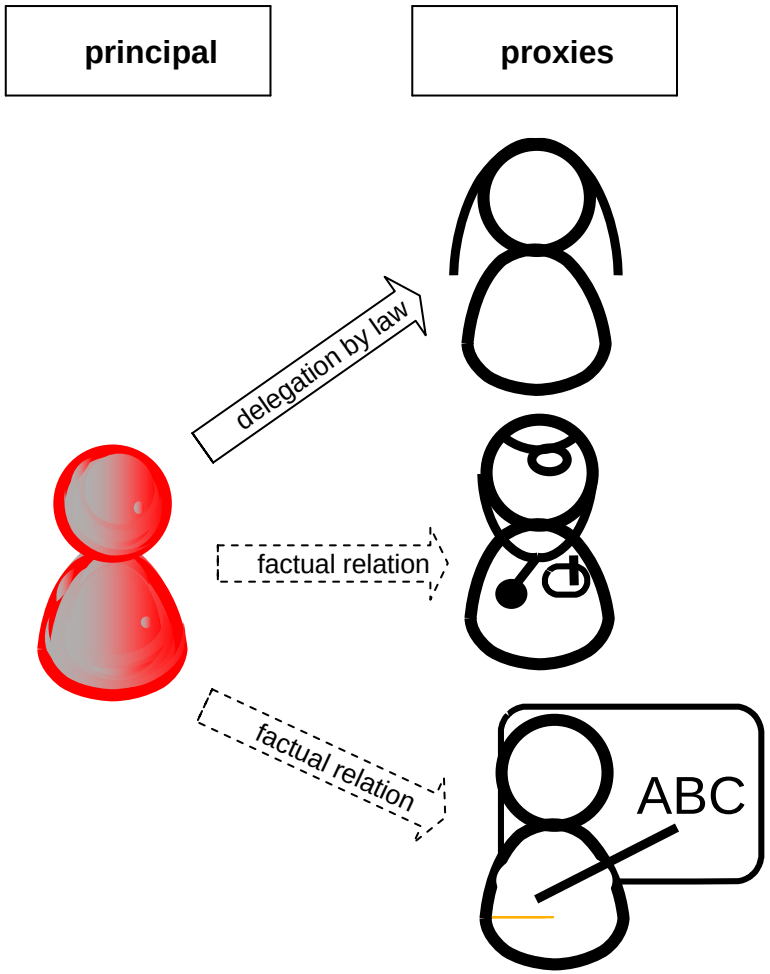
- DNA information
- hereditary diseases
- social relations

solutions

⇒ enforcement by parents

⇒ legal regulations required as guideline, providing minimum protection

childhood



challenges

- double role of parents (proxy and data controller)
- other proxies for specific pIDs (doctors, teachers, coach), legal treatment as controllers?

solutions

- guideline: best interest
- account for growing autonomy
- listen carefully for preferences
- verify consent after maturity

in general: lacking capability

persons lacking capability to manage their privacy

- rules as for children apply: listen for preferences, taking level of capability into account
- legally relevant actions: privacy issues are covered by the agent [law] power of attorney
- real actions: principal should be enabled to decide on usage of personal data or be allowed to select a proxy for privacy issues

tomb

deceased persons

starting point

- deceased persons are not considered data subjects by the law anymore. But: “post-mortal personality right”
  - law of succession: heir steps in all contractual relations
  - who should enforce privacy? conflicting interests

options

- service providers could offer options
- choosing a “privacy proxy” for the post-mortal period

legal requirements

- delegation in privacy matters must be recognised by law
- proxies should act under an own (partial) identity
- control of the principal: access to own tamper-proof but transitive data collection
- protection of the proxy, nevertheless: clear liability rules
- specific legal requirements (e.g., for minors, incapable persons giving guidance for cases of doubt)

practical requirements

- technological representation of delegation (from issuance to revocation) is needed
- principal's credentials must not be used by proxy
- logging / data track (both principal and proxy)
- means to express preferences, guidelines, conditions
- possibly: access to principal's data track to choose pID
- protection of the proxy's privacy (minimisation, deletion)

“Vacation in Wolf Land”

Thank you for your attention

contact:
Harald Zwingelberg
ULD65@datenschutzzentrum.de
www.datenschutzzentrum.de
+49 (0)431 / 988-1228