Data Protection and Ethics in Healthcare

Harald Zwingelberg
ULD

June 14th, 2017
at Brocher Foundation, Geneva

Organized by: with input by:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Overview

- Goal: Protection of people
- Specific legal setting for medical data
- Security and Privacy protection goals
- Recap and conclusion

- This had been topic at Geneva meeting? =>

Topic at CANVAS Workshop Geneva

Data protection is about ~~data~~

Foto: Ashtyn Renee

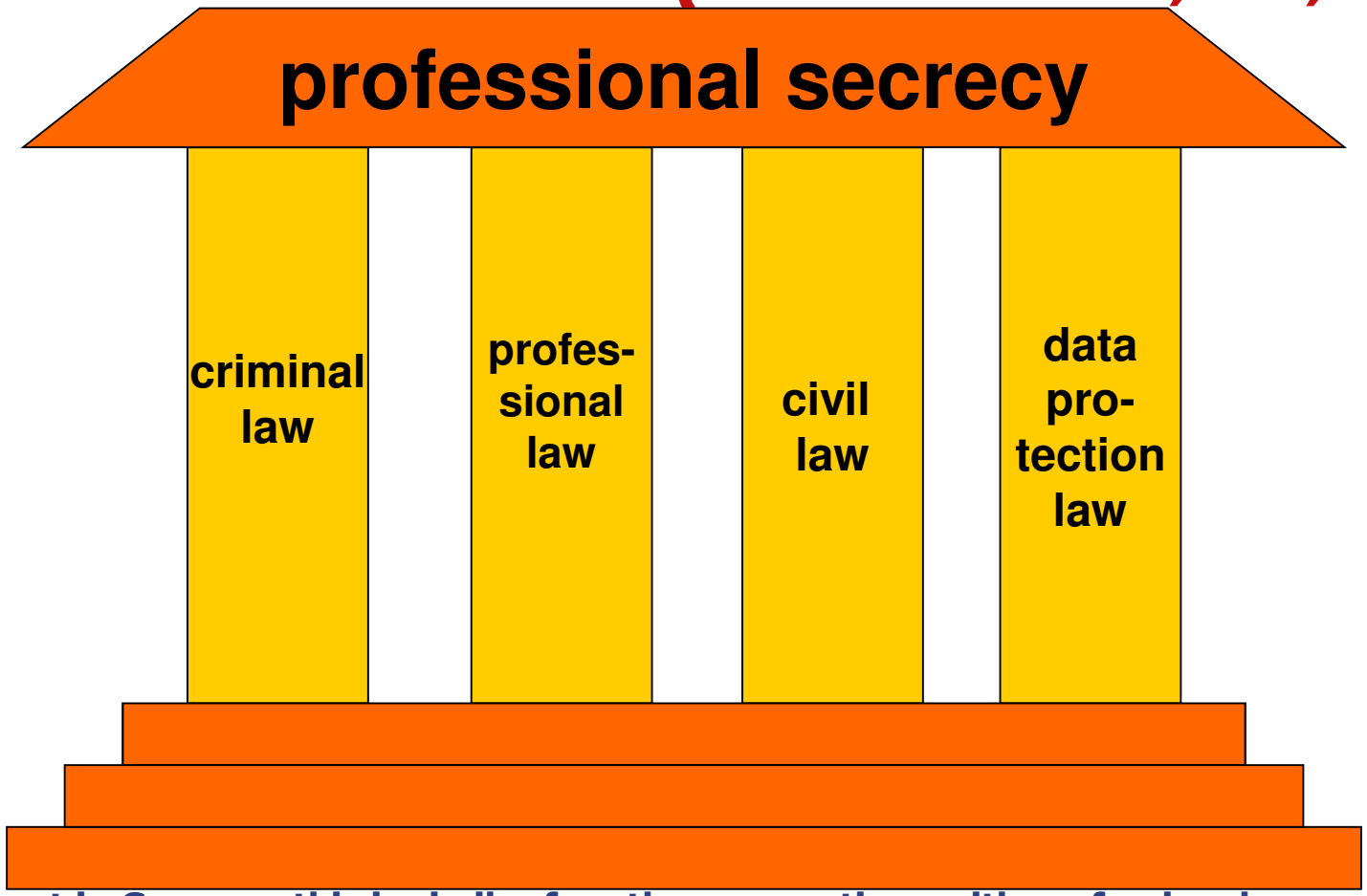
people and their fundamental rights

To be checked while developing technologies for connected cars

- impact on persons
- impact on society

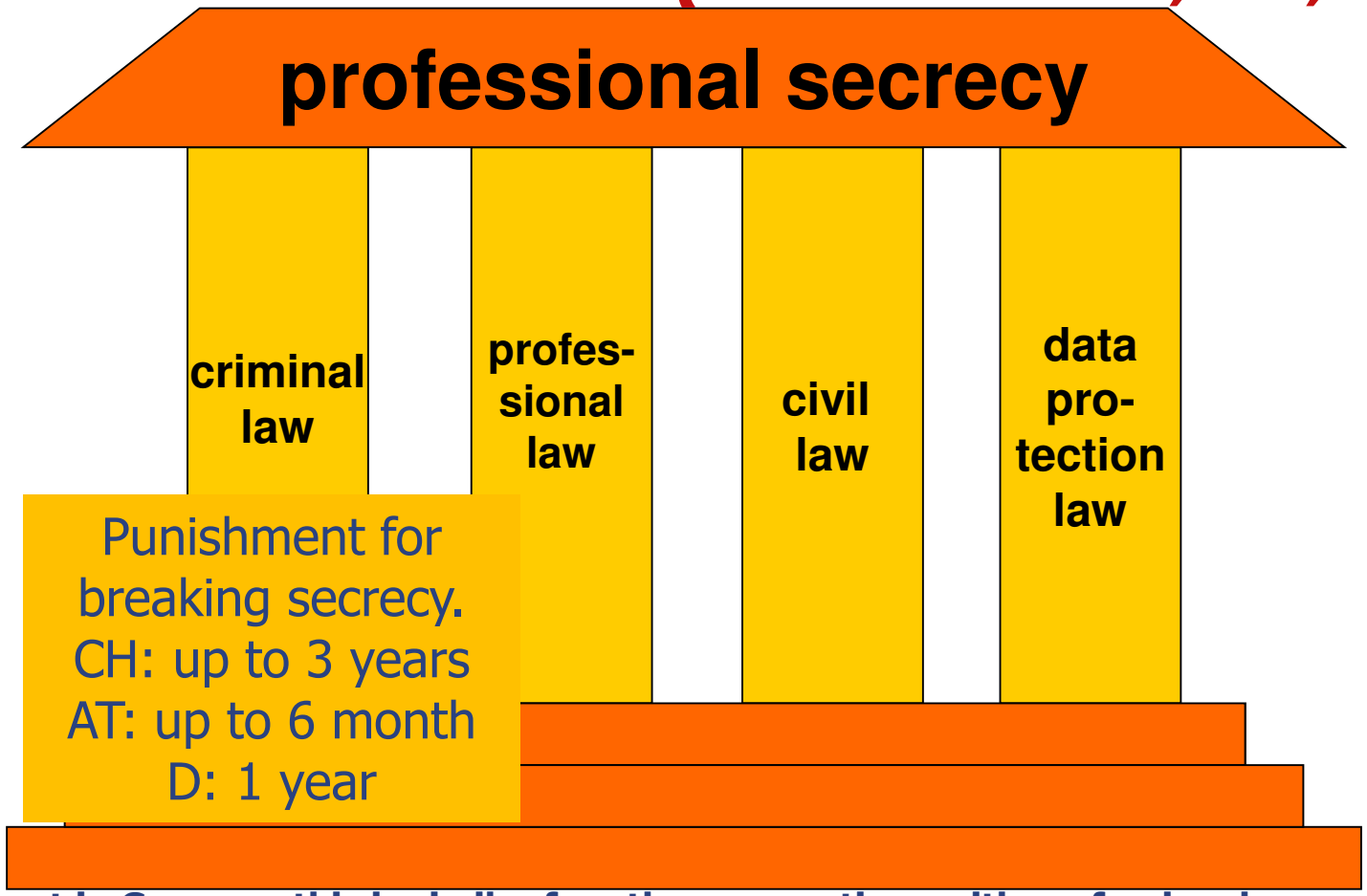
Topic at CAMVAS Workshop Geneva

*Protection of Medical data (verified for D, AT, CH)**



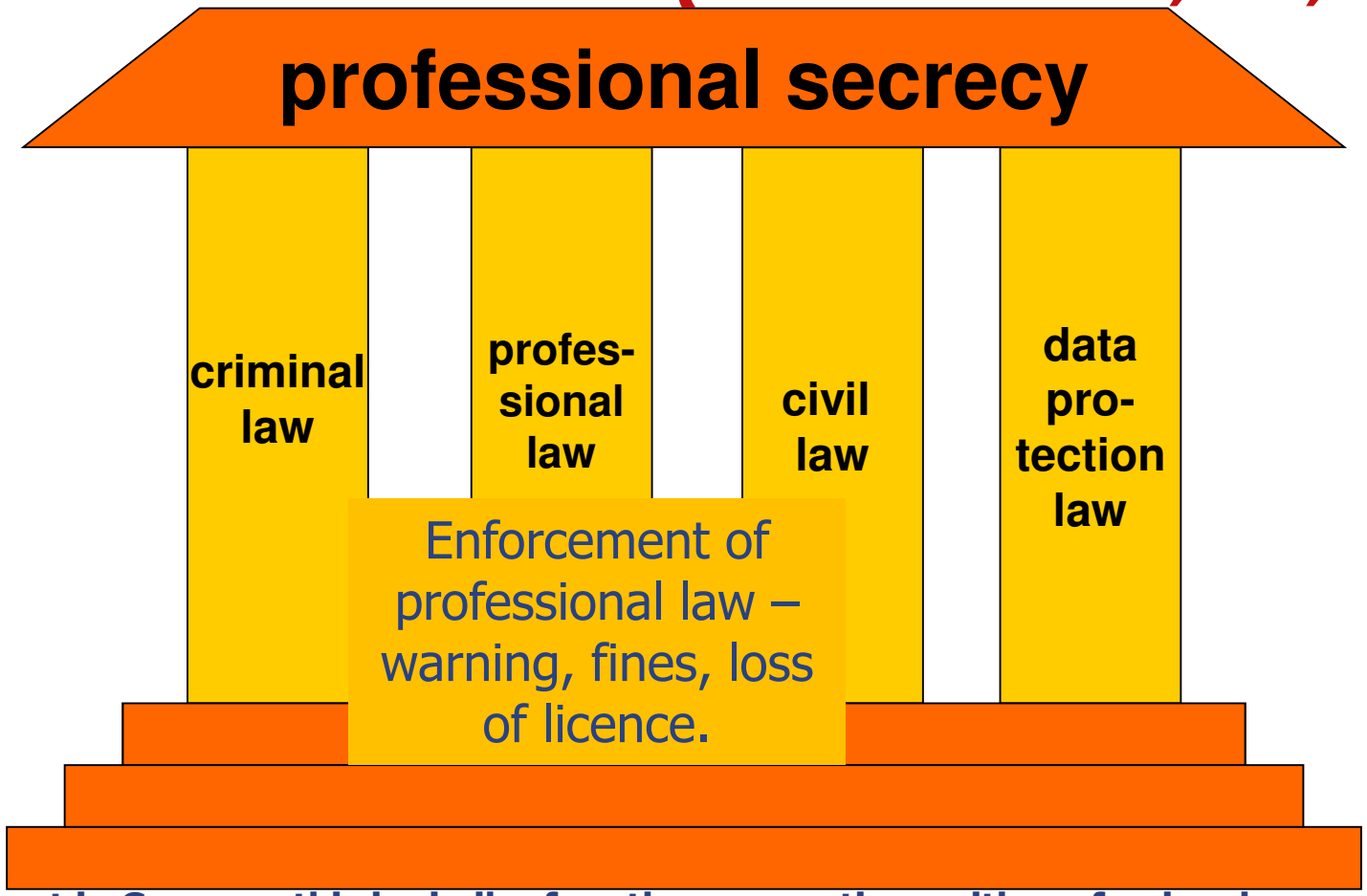
- **At least in Germany this is similar for other occupations with professional secrecy including other medical professions such as dentists, apothecaries, psychologists but also advocates, notaries, tax consultants, etc.**

*Protection of Medical data (verified for D, AT, CH)**



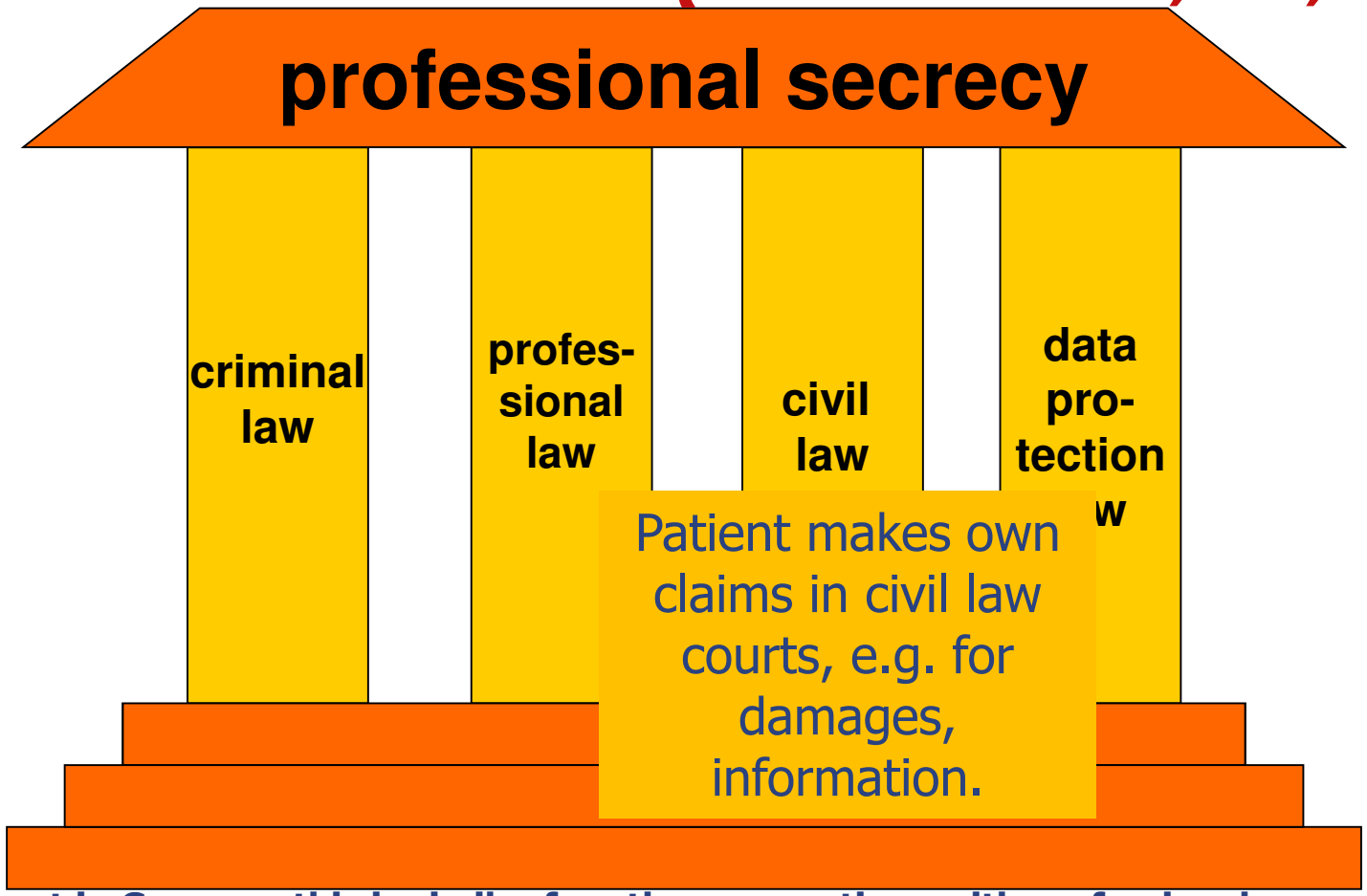
- **At least in Germany this is similar for other occupations with professional secrecy including other medical professions such as dentists, apothecaries, psychologists but also advocates, notaries, tax consultants, etc.**

*Protection of Medical data (verified for D, AT, CH)**



- **At least in Germany this is similar for other occupations with professional secrecy including other medical professions such as dentists, apothecaries, psychologists but also advocates, notaries, tax consultants, etc.**

*Protection of Medical data (verified for D, AT, CH)**



- **At least in Germany this is similar for other occupations with professional secrecy including other medical professions such as dentists, apothecaries, psychologists but also advocates, notaries, tax consultants, etc.**

*Protection of Medical data (verified for D, AT, CH)**

professional secrecy

Reasoning:
Protection of the doctor-patient relationship. Patients must feel their data to be save and secure with the health provider to have trust. Otherwise necessary information may be withheld and cause threat to success of treatment and patient safety.

Topic at CAMVAS Workshop Geneva

data pro-tection law

General rules and specific requirements for special categories of data – genetic, biometric and health data

- **At leas… cy**
  includ… ts but
  also a…

Protection of Medical data (verified for D, AT, CH)*

- So far strict rules on medical data, specifically enforced as professional secrecy

- Opening clause in Art. 90 GDPR for member states to adopt specific regarding the enforcement of obligations of professional secrecy

⇒ Remains to be seen how members states react

⇒ Highly relevant for the health sector as professional secrecy applies to physicians and many healthcare professionals

Security Protection Goals

Confidentiality

"The protection goal of

Confidentiality

is defined as the property that

(privacy-relevant) data

and services that process such data

cannot be accessed

by unauthorized entities."

Confidentiality applied to helath data

- **Protection of patients data**
- **Separation of data necessary for different tasks / roles, separation of different**
- **Even the information, that health related or AAL devices exist in a household is subject to confidentiality**
- **Timely deletion of unnecessary data**

Confidentiality

Implementation Techniques:

- **Data Encryption**
  - **in transit (TLS, HTTPS, SSH, …)**
  - **at rest (PGP, S/MIME, TrueCrypt, …)**
  - **Encryption special to national health record system**
  - **…**
- **Data Segregation**
  - **Secret Sharing, Secure Multiparty Computations**
- **Access Control Enforcement**

Integrity

"The protection goal of

Integrity

is defined as the property that

(privacy-relevant) data

and services that process such data

cannot be modified in an unauthorized

or undetected manner."

Integrity for health data

- **Access to unchanged and accurate information in health files**
- **Detect unauthorized changes**
- **What if ransomware randomly changes values in patient files?**
- **Protection of access and medical devices e.g. for pacemakers, insulin pumps**

Integrity

Implementation Techniques:

- **Digital Signatures**
- **Hash Values**
- **Access Control Enforcement**

- **Low energy cryptography for implantable devices**

Availability

"The protection goal of

Availability

is defined as the property that

access to (privacy-relevant) data

and to services that process such data

is always granted

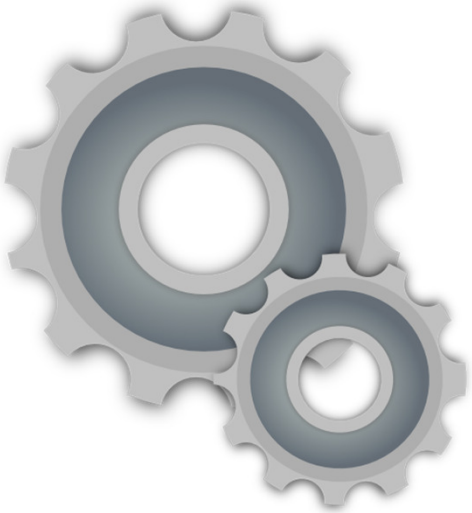
in a comprehensible, processable, timely manner."

Availability for health data

- **Have data available when needed**
- **Processes for loss of data (Backups)**
- **Accessibility when and where necessary (mobile access, home visits)**

Availability

Implementation Techniques:



- **Backups**
- **Load Balancers**
- **Failovers**
- **Redundant Components**
- **Avoidance of Single-Points-of-Failure**
- **Watchdogs / Canaries**

Privacy Protection Goals

Unlinkability

"The protection goal of

Unlinkability

is defined as the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context."

Unlinkability for health data

- **Central health records: measures against forcing patients into giving away the data e.g. plausible deniability**

Topic at CANVAS Workshop Geneva

- **Use of pseudonyms in research and allow identity management**
- **Well considered architecture decisions, e.g. between centralized / cloud based solutions vs. decentralized user-controlled systems**

Topic at CANVAS Workshop Geneva

Unlinkability for health data

- **Research databases: share unlinkable data (e.g. based on concepts such as k-anonymity, l-diversity etc.)**
- **Research databases: multiparty computation**
- **Research databases: publication of aggregated data only**

Topic at CANVAS Workshop Geneva

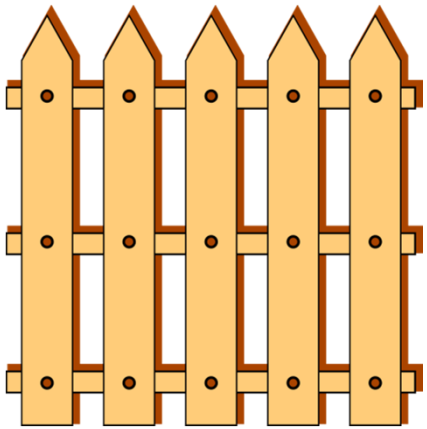
Unlinkability

Implementation Techniques:

- **Data Avoidance / Reduction**
- **Access Control Enforcement**
- **Aggregated data**
- **Separation / Isolation**
- **Avoidance of (unique) Identifiers**

Unlinkability

Think of it as …



Transparency

"The protection goal of

Transparency

is defined as the property that

all privacy-relevant data processing

–including the legal, technical,

and organizational setting–

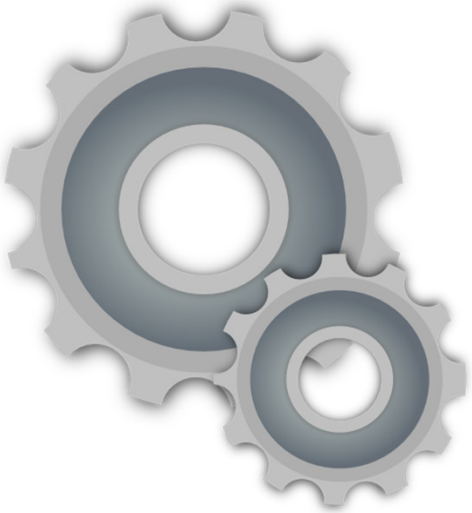
can be understood and reconstructed at any time."

Transparency for health / ambient assisted living

- **Information must be understandable and "digestible" for target audience**
- **For digital screens: scalable text, no ads that can hide the information**
- **Multi-layered policies with pictures and diagrams**
- **Computer readable privacy policies**
- **Understandable controls e.g. I/O buttons**

Transparency

Implementation Techniques:



- **Logging and Reporting**
- **User notifications**
- **Documentation of services**
- **Privacy policies**
- **Transparency Services for patient files**
- **(useful) Data breach notifications**

Transparency

Think of it as …

Intervenability

"The protection goal of

Intervenability

is defined as the property that intervention is possible concerning all ongoing or planned privacy-relevant data processing."

Intervenability

- **Control in hands of the patients, e.g. allowing interruption of surveillance and tracking e.g. for monitoring devices in sports, in ambient assisted living granting moments of privacy**
- **Design: Address special requirements of target audience (sick, injured, elderly, or confused persons)**

Topic at CAMVAS Workshop Geneva

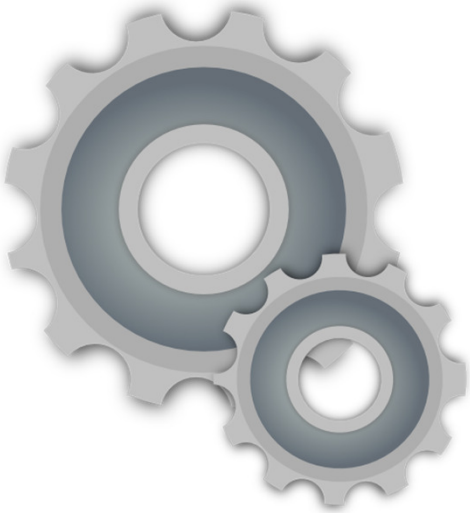
Intervenability

- **Provide transparency and way for informed consent / right to object for any change of purposes and secondary use of data.**
- **Quality of life: Allow patients to stay at home and provide necessary aid when necessary.**

Topic at CANVAS Workshop Geneva

Intervenability

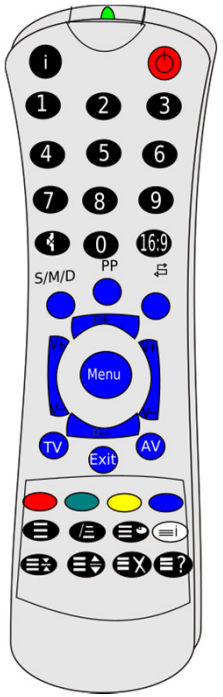
Implementation Techniques:



- **Configuration Menu**
- **Help Desks**
- **Stop-Button for Processes**
- **Break-Glass / Alert Procedures**
- **Manual Override of Automated Decisions**
- **External Supervisory Authorities (DPAs)**

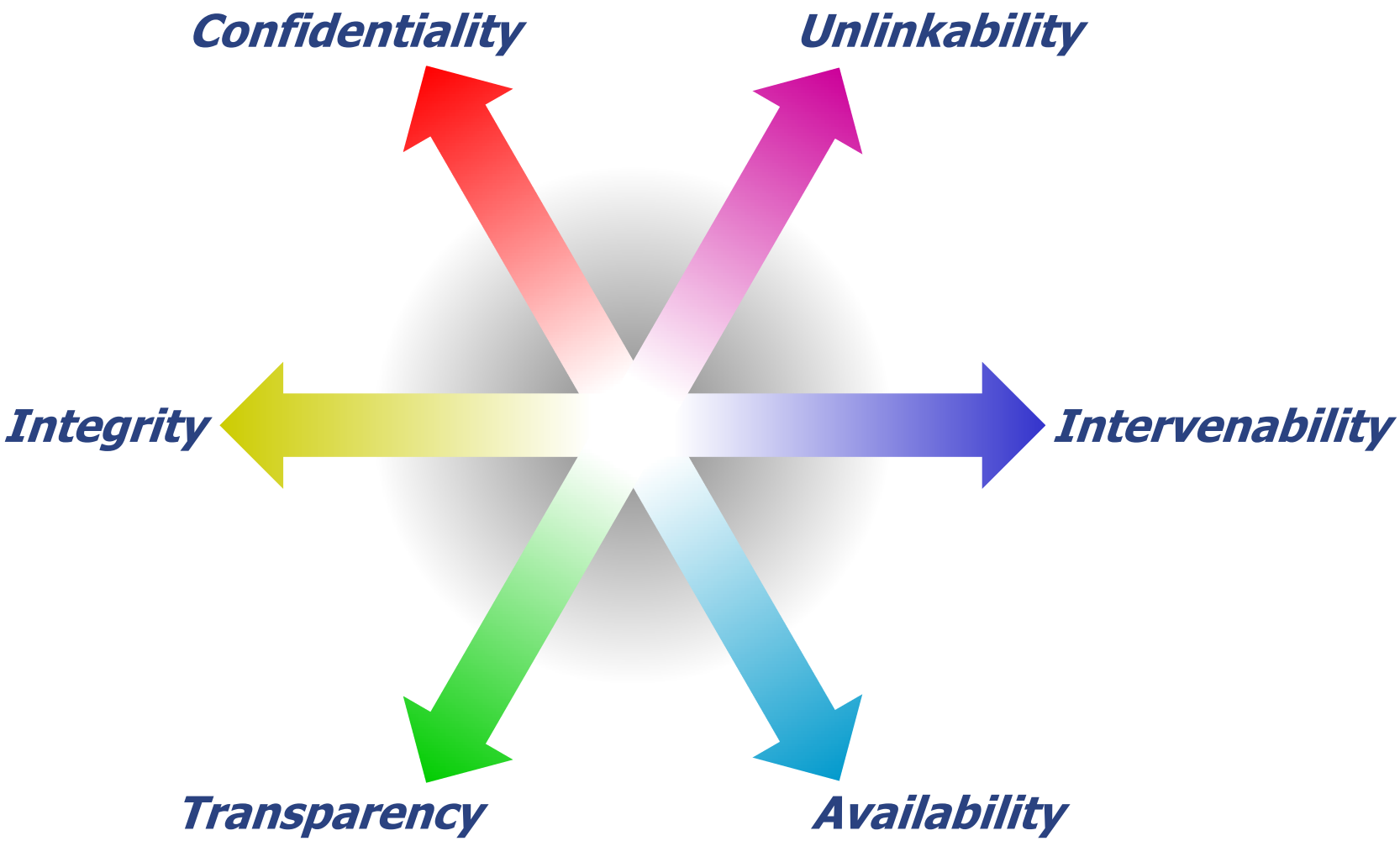
Intervenability

Think of it as …

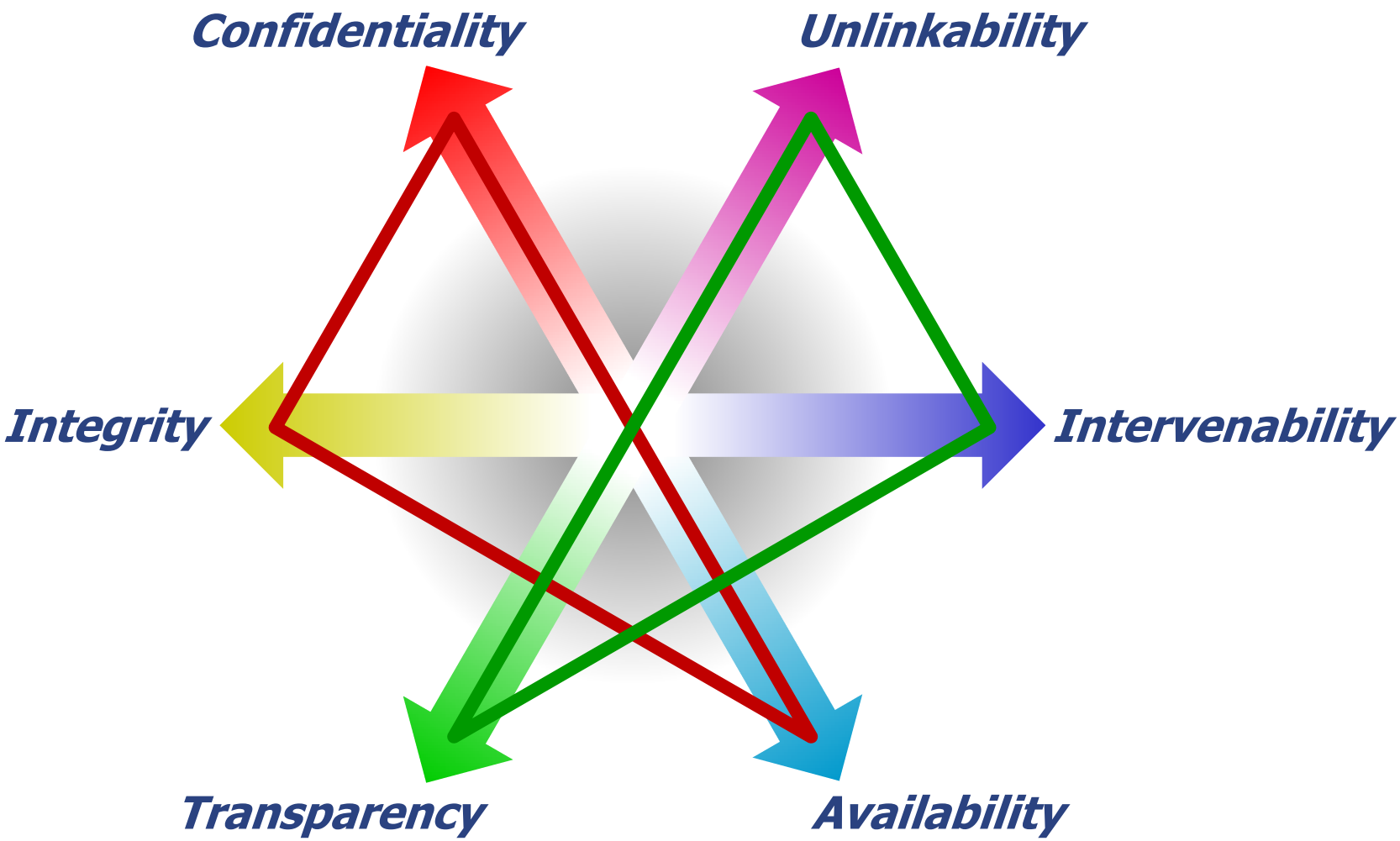


The whole picture

Data protection goals



Data protection goals



Data protection goals

Conclusion

Conclusion

- **Protection Goals have proven very useful**
- **How to bring ethics and privacy to practice?**
  - **Insert in existing testing and evaluation processes**
    - **Include ethic aspects in privacy assessments by DPO s/ DPA**
    - **Consider privacy aspects in assessments by ethic boards**
  - **Construction of an additional protection goal, but if so – what could it be**
  - **Include ethic aspects into other assessment steps:**
    - **Weighing process of legal ground, e.g. as "suitable safeguard for rights and freedoms" or "proportionate processing" (Art. 9 GDPR)**
    - **Mandatory consideration points in public calls for tenders by hospitals, social security and health insurances**

Conclusion (last minute slide)

- **Suggestion for a statement in the paper on this conference:**
  Make security, data protection and ethical aspects integral part of investment decisions.
  Make it mandatory where possible (public health insurance, all investments and call for tenders by public bodies such as university and municipal hospitals).
  Entry points in Art. 32 and 25 GDPR

More about the Standard Data Protection Model

- Content
  - Methodology
  - Data Protection Goals
  - In progress: catalogues with measures
- V.1.0 recommended for intensified testing by the conference of German data protection authorities.
- One of three existing DPIA frameworks (Fr, GB, D) mentioned by Art. 29 WP in working paper 248 in April 2017.


SDM
Standard-Datenschutzmodell

Das Standard-Datenschutzmodell

Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele

V.1.0 – Erprobungsfassung

von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen
(Enthaltung durch Freistaat Bayern)

Latest versions and translations are and will be available at:

https://www.datenschutzzentrum.de/sdm/

Data Protection in Ambient Assisted Living (2011)

- Content
  - Early evaluation of the whole upcoming branch of ambient assisted living technologies (AAL)
  - Structured on basis of the data protection goal methodology
  - Data protection requirements
  - Research questions

German version only:

https://www.datenschutzzentrum.de/projekte/aal/

Funding Notice

Slides are based on results from CANVAS and these further projects:

Forum Privatheit I & II

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

funded by the German Federal Ministry of Education and Research

www.forum-privatheit.de/

SPECIAL

European Commission

Funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 731601

specialprivacy.eu

Privacy & Us

European Commission

funded by MSCA-ITN-2015-ETN – Marie Skłodowska-Curie Innovative Training Networks Project Number: 675730

www.privacyus.eu

Thank you for your attention
Questions? Comments?

Harald Zwingelberg

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

https://www.datenschutzzentrum.de/projekte/canvas/

E-Mail: uld6@datenschutzzentrum.de

Phone: +49 431 988-1222

Funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 700540