

# ***PROTECTION GOALS FOR PRIVACY ENGINEERING***

Marit Hansen, Meiko Jensen, and Martin Rost

International Workshop on Privacy Engineering


May 21, 2015

# *Outline*

- 
- **Security Protection Goals**
  - **Privacy Protection Goals**
  - **Three Axes**
  - **Conclusion**

# 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*

*...in other words:*

- **Secrecy**
- **Non-Disclosure**
- **Access Restrictions**
- **Security Clearances**
- **Data Minimization**
- **Steganography**
- **Unobservability**

# *Confidentiality*

## Implementation Techniques:

- **Data Encryption**
  - in transit (TLS, HTTPS, SSH, ...)
  - at rest (PGP, S/MIME, TrueCrypt, ...)
  - ...
- **Data Segregation**
  - Secret Sharing, Secure Multiparty Computations
  - Onion Routing
- **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*

*...in other words:*

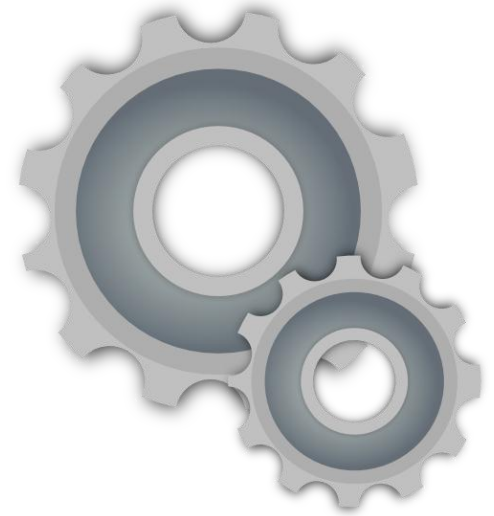
- Authenticity
- Detection of Data Changes
- Non-Repudiation
- Reliability



## *Integrity*

### Implementation Techniques:

- **Digital Signatures**
  - RSA, ElGamal
  - Message Authentication Codes
  - ...
- **Hash Values**
- **Access Control Enforcement**
- **Watchdogs / Canaries**
- **Two-Man Rules**



## ***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***

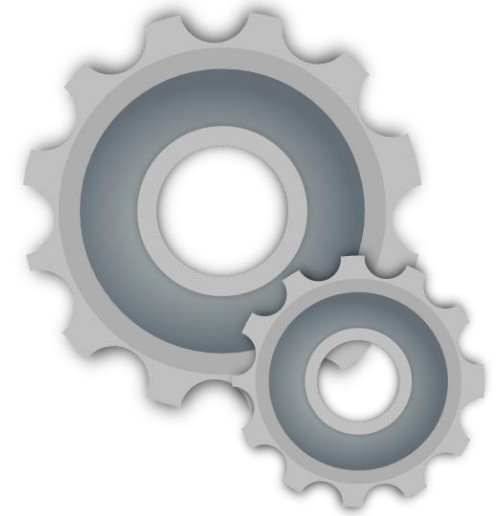
*...in other words:*

- Redundancy
- Monitoring of Availability
- Responsiveness
- Accessibility
- Uptime

## *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*

*...in other words:*

- Data Minimization
- Necessity / Need-to-Know
- Purpose Binding
- Separation of Power
- Unobservability
- Undetectability

# *Unlinkability*

## Implementation Techniques:

- **Data Avoidance / Reduction**
- **Access Control Enforcement**
- **Generalization**
  - **Anonymization/Pseudonymization**
  - **Abstraction**
  - **Derivation**
- **Separation / Isolation**
- **Avoidance of Identifiers**

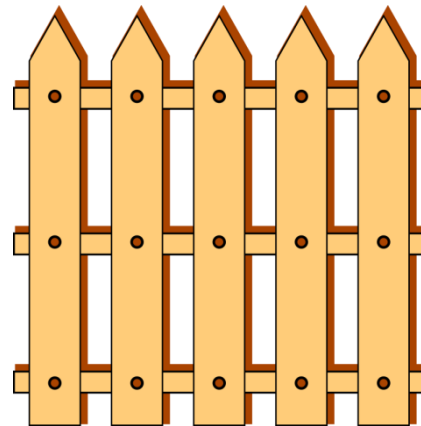




# *Unlinkability*



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*

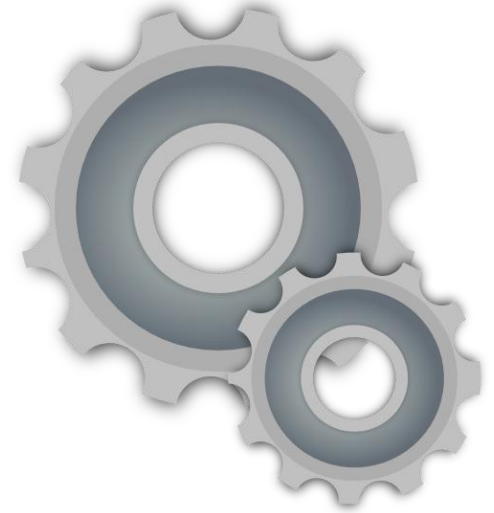
*...in other words:*

- Openness
- Accountability
- Documentation
- Reproducibility
- Notice (and Choice)
- Auditability
- Full-Disclosure

## *Transparency*

### Implementation Techniques:

- **Logging and Reporting**
- **User Notifications**
- **Documentation**
- **Status Dashboards**
- **Privacy Policies**
- **Transparency Services for Personal Data**
- **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***

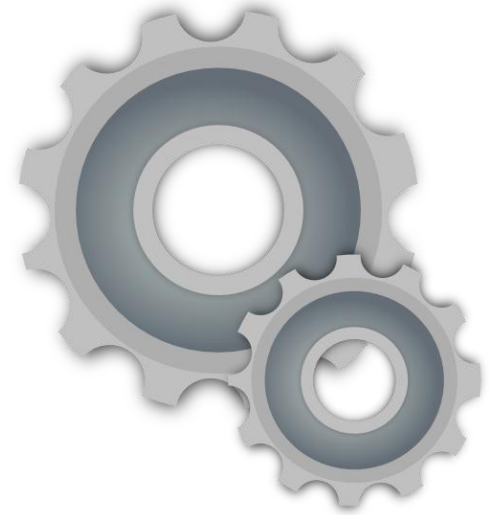
*...in other words:*

- Self-determination
- User Controls
- Rectification or Erasure of Data
- (Notice and) Choice
- Consent Withdrawal
- Claim Lodging / Dispute Raising
- Process Interruption

# *Intervenability*

## Implementation Techniques:

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

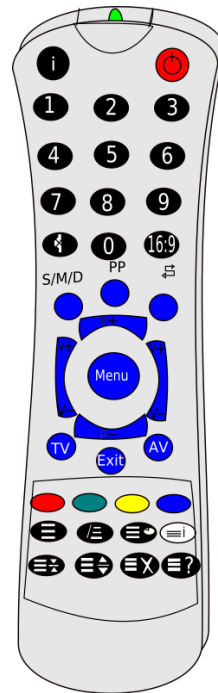




# *Intervenability*

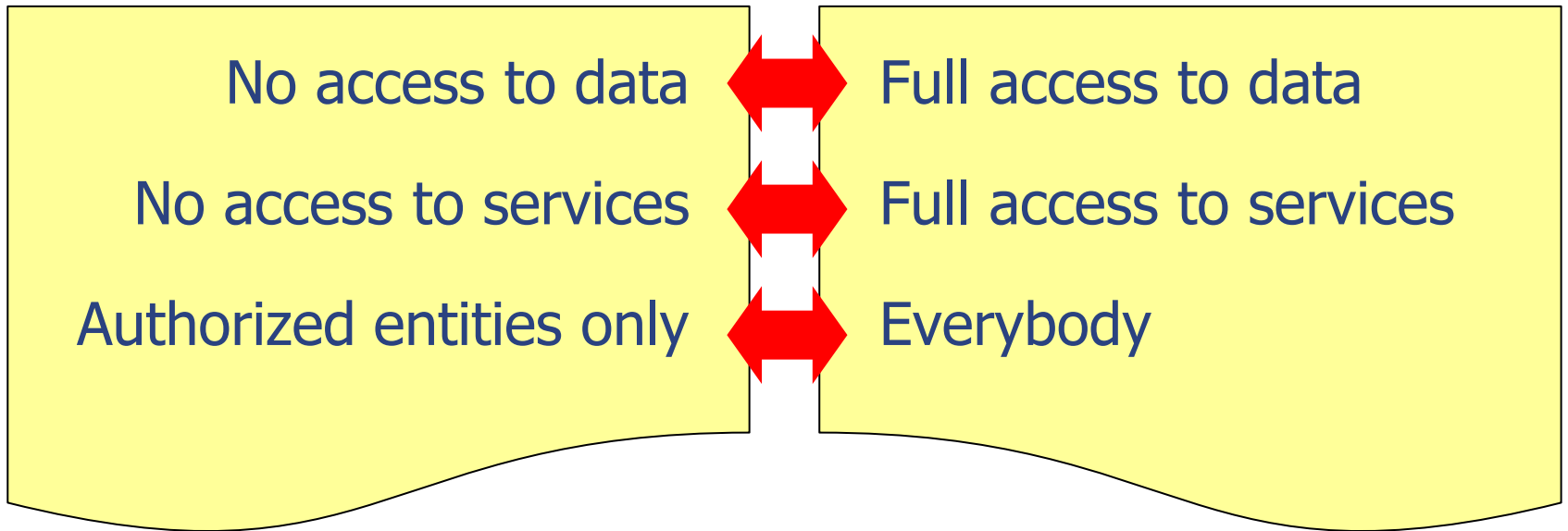


Think of it as ...



# Three Axes

# *Confidentiality <-> Availability*

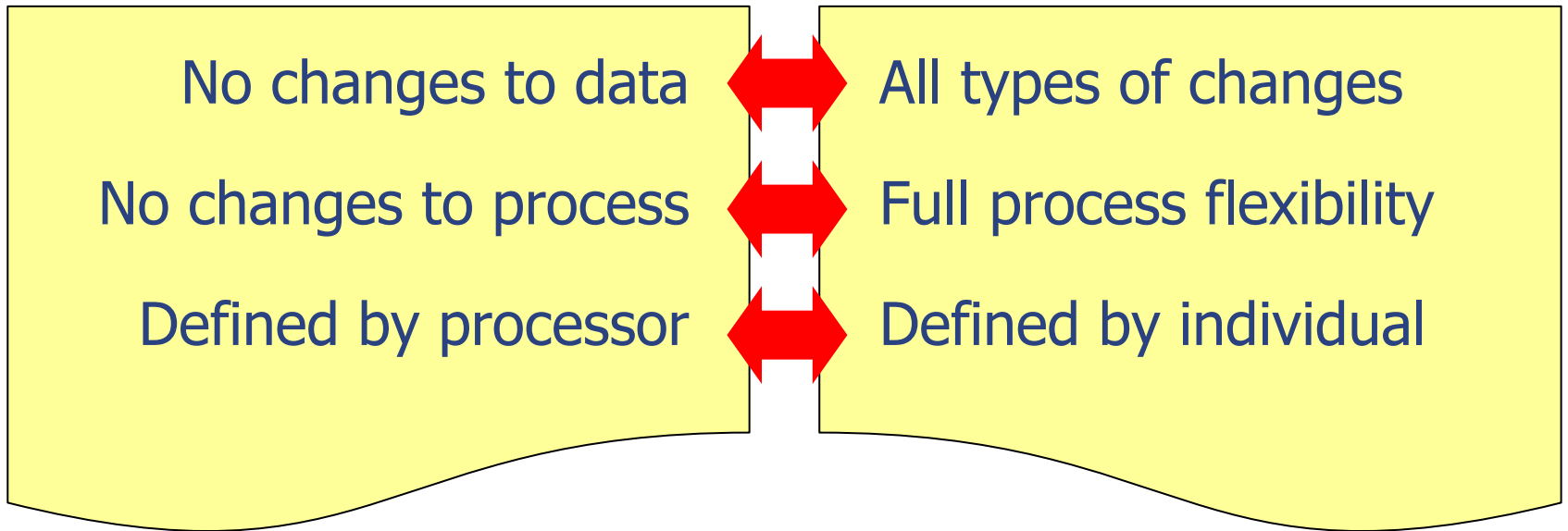


***Confidentiality***

***Availability***



# *Integrity <-> Intervenability*

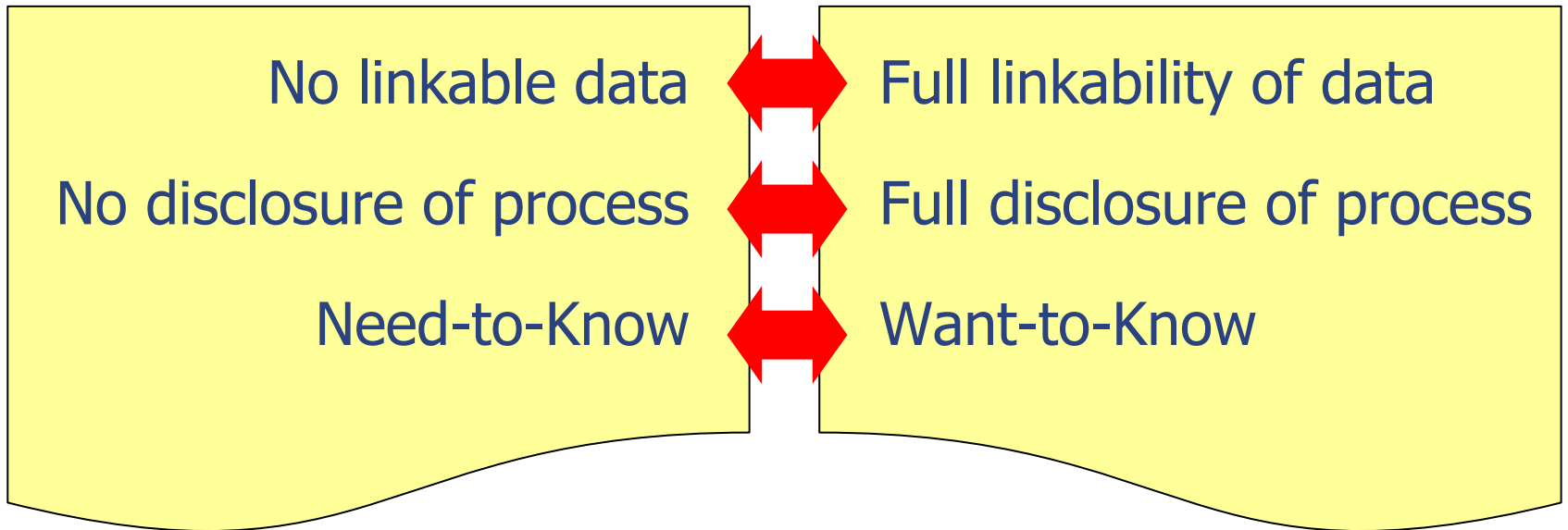


***Integrity***

***Intervenability***



# *Unlinkability <-> Transparency*

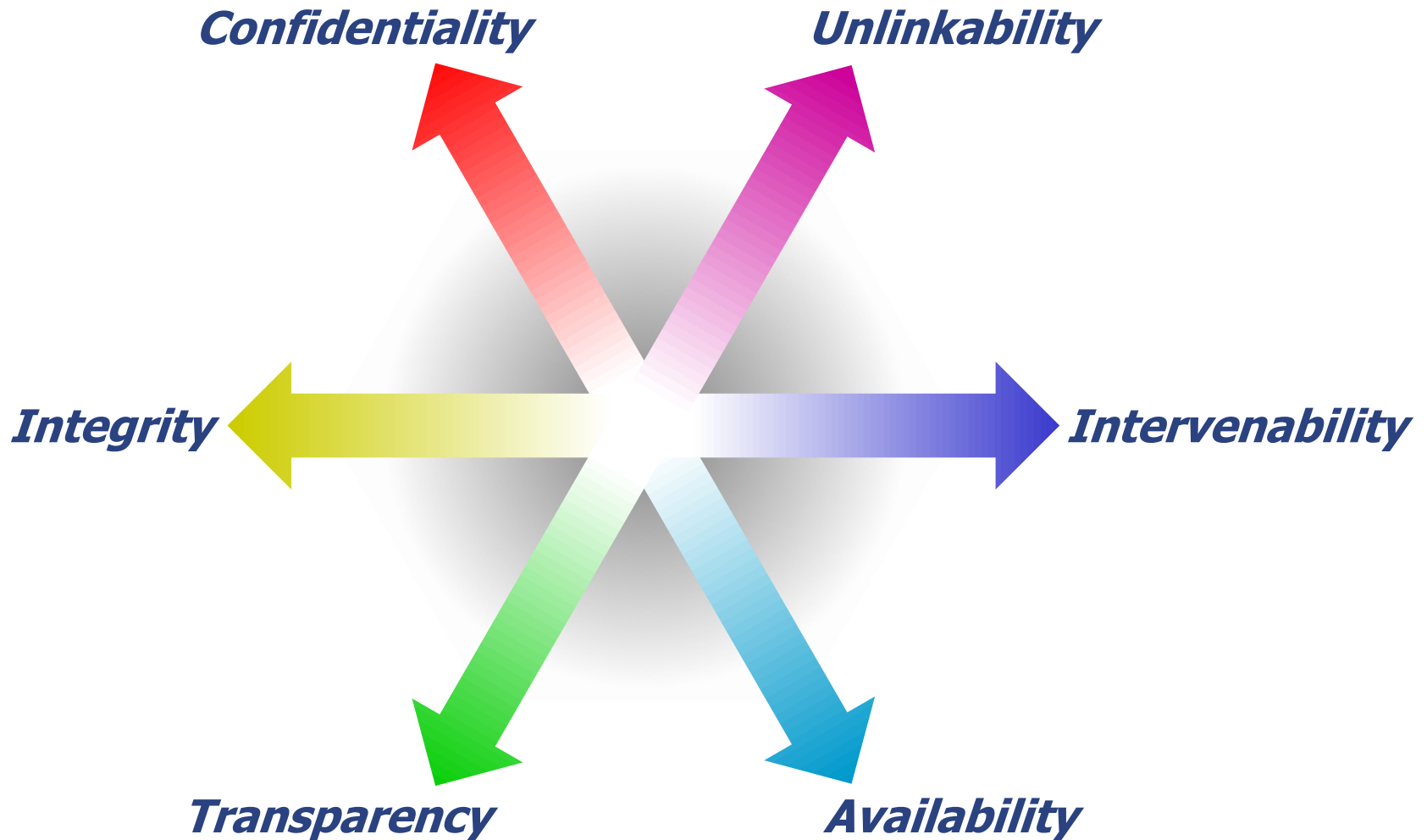


***Unlinkability***

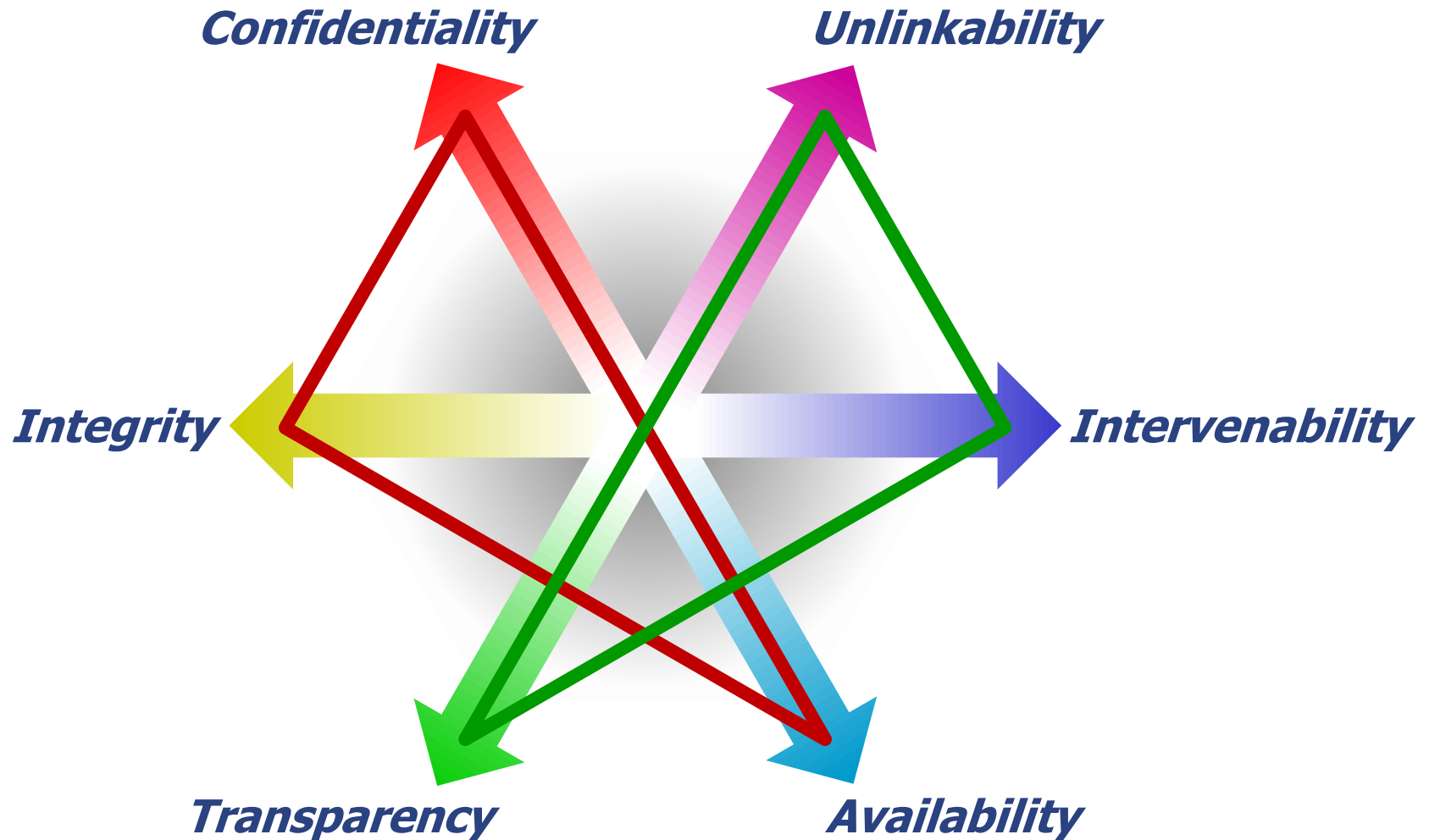
***Transparency***



# *The Six-Pointed Star*



# *The Six-Pointed Star*

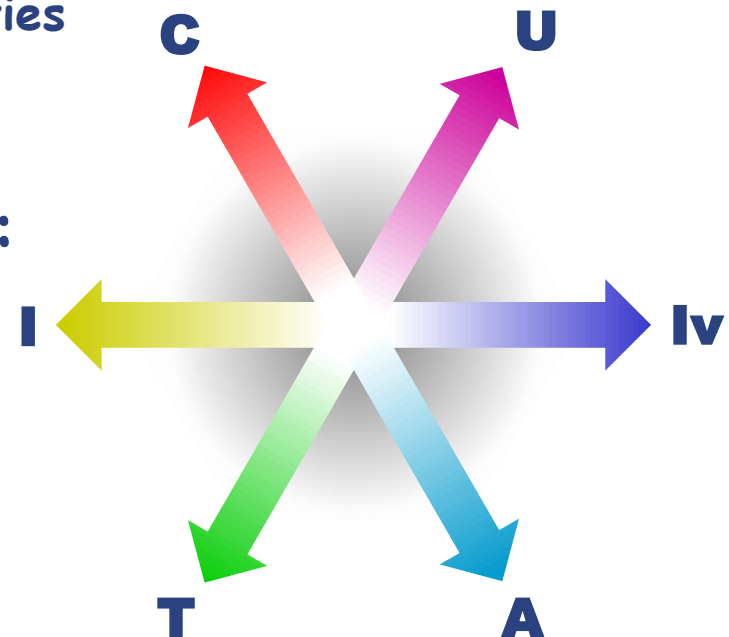


# Conclusion



## Conclusion

- Protection Goals have proven very useful:
  - for Implementers
  - for Lawyers
  - for Data Protection Authorities
  - for Users
- Privacy Protection Goals:
  - Unlinkability
  - Transparency
  - Intervenability



## References



*Shaping the Future  
of Electronic Identity*

partly funded by  
EU FP7,  
GA n° 318424



[www.futureid.eu](http://www.futureid.eu)



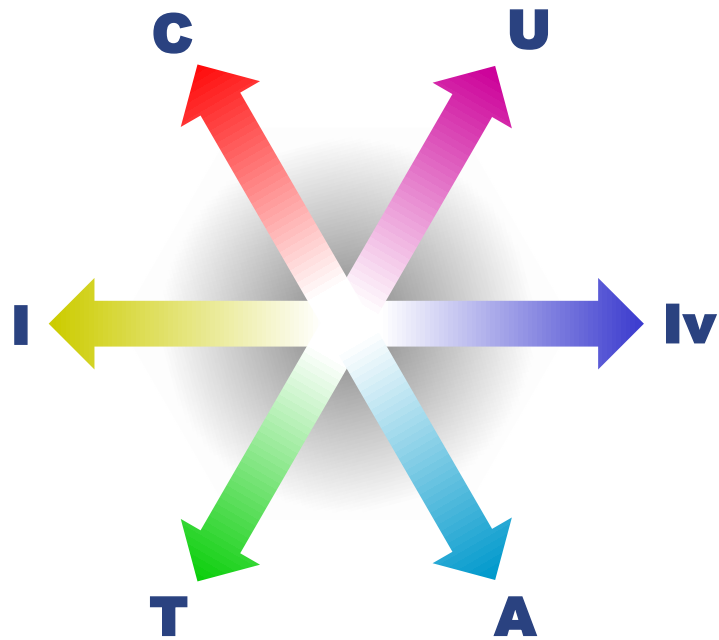
*Forum Privatheit  
und selbstbestimmtes Leben  
in der Digitalen Welt  
(Privacy Forum Germany)*



partly funded by the  
German Federal Ministry  
of Education and Research

[www.forum-privatheit.de](http://www.forum-privatheit.de)

***Thank You!***



**Protection Goals  
for Privacy Engineering**

Marit Hansen,  
Meiko Jensen,  
and Martin Rost

Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein  
Phone: 0431 988 – 1200  
uld6@datenschutzzentrum.de  
<http://www.datenschutzzentrum.de/>



Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein