Privacy by Design with or without information security?

Kirsten Bock

CPDP 01-23-2013

EuroPriSe
European Privacy Seal

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ULD Seals

- Facilitating compliance with German + SH dp law
- Privileged in public procurement in SH
- 2003-2012: 76 Certificates

European Privacy Seal

DE-12301 / Valid 2010-08

- Facilitating compliance+ with EU dp regulations with regard to national law
- 2008-2012: 21 Certificates

Advantages of Certification

- Completes documentation
- Provides third party assurance
- Proves compliance (B2B)
- Creates a unique selling preposition
- Keep up with competition

➔Privacy can be a market niche

Promoting PET solutions

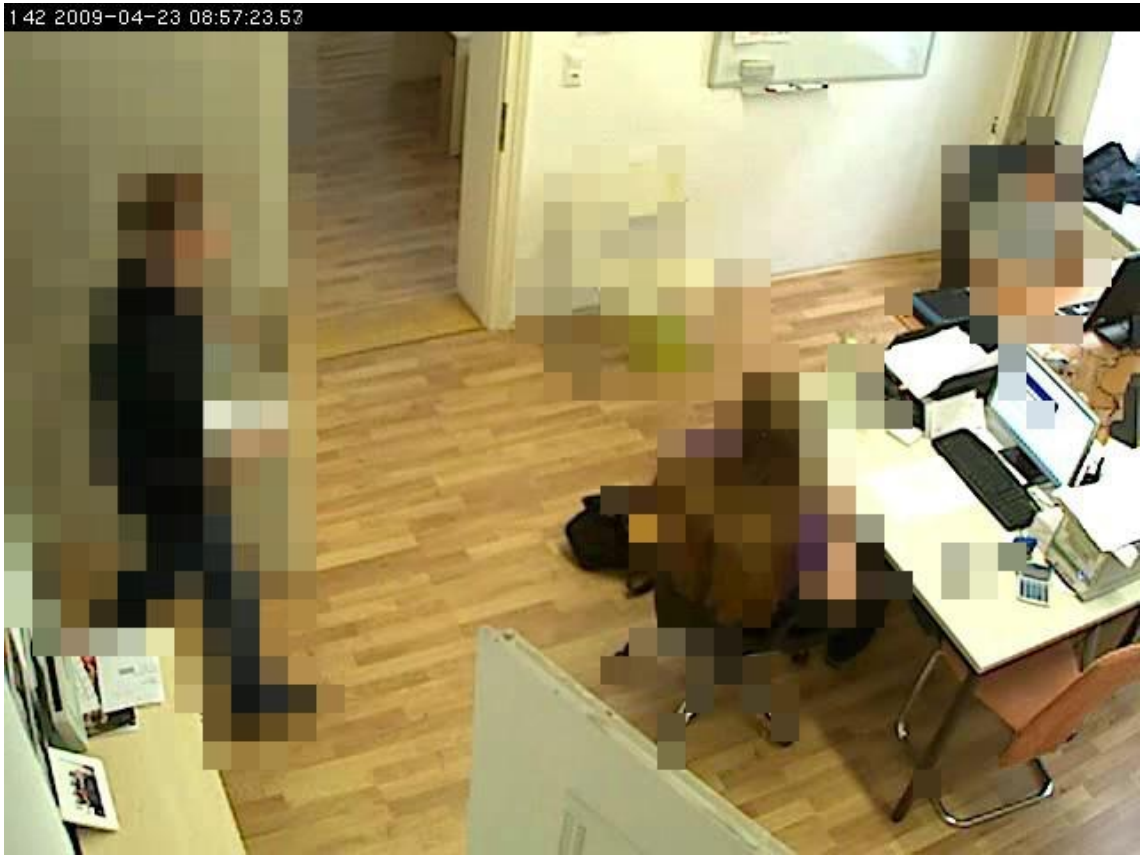
Example:

KiwiVision (08/2009)

Privacy Protector,

Software module for integration in a video management system

Version 1.0



https://www.european-privacy-seal.eu/awarded-seals/de-090017

PbD in IT Security

Privacy by Design

=

Managing the organisation of IT security with respect to safeguarding the fundamental right of data protection

Risk focus is on how organisations deal with PII of employees, members, citizens, customers, patients, “humans”

Make PbD an Obligation

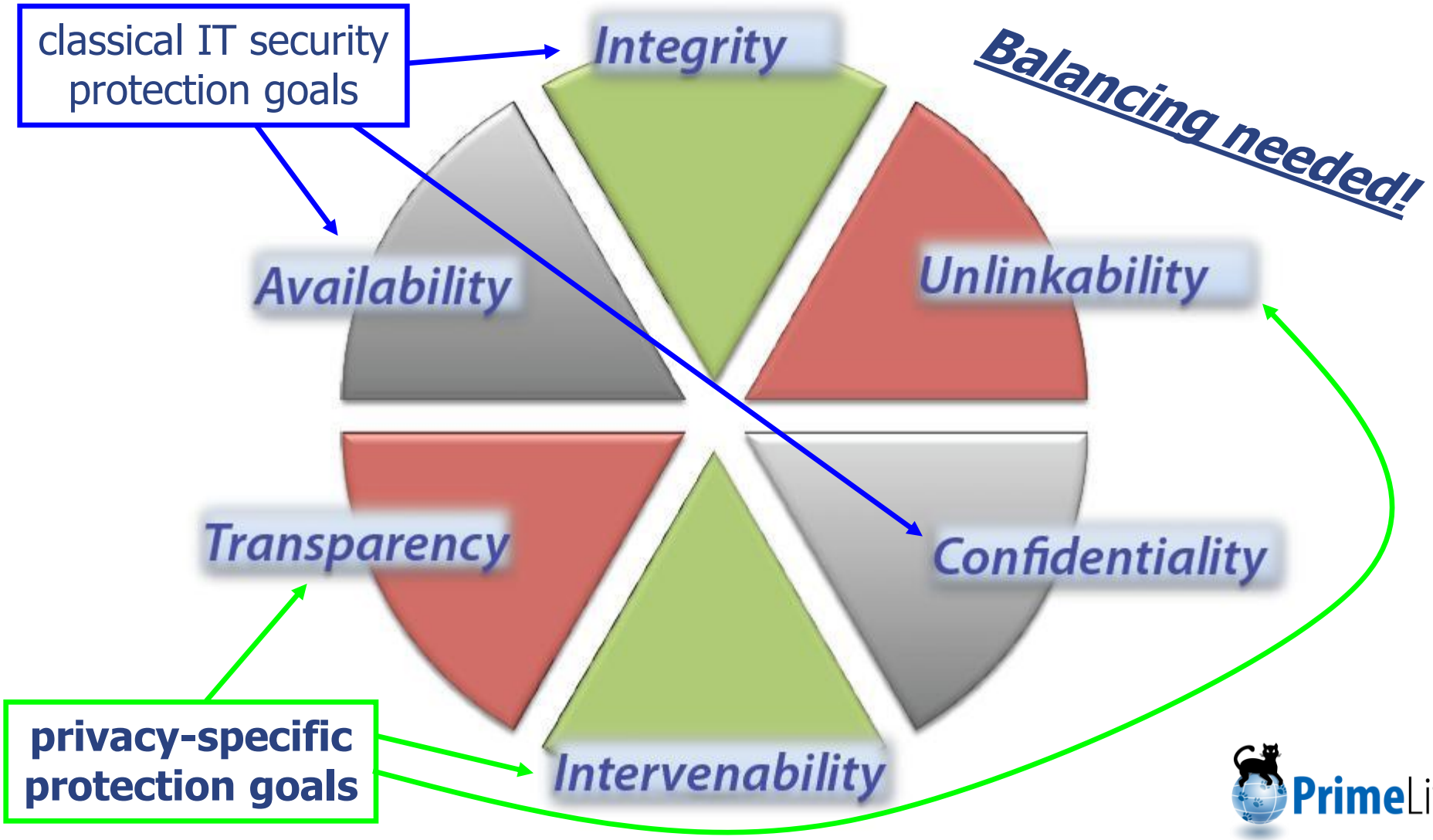
Often technical solutions are

- build to serve motives/business models
- Do not take legal dp requirements into account
- Motives are biggest data protection problem

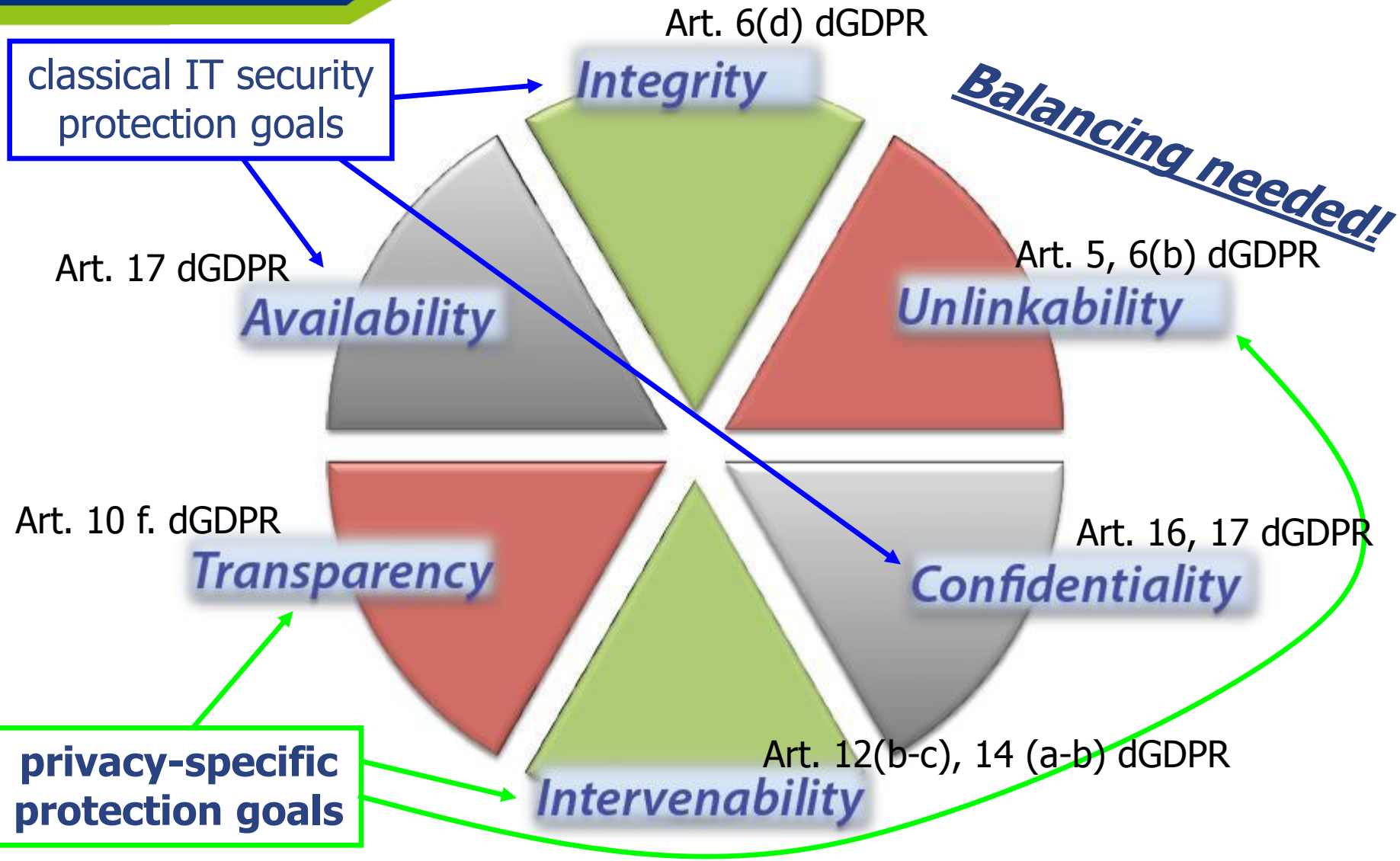
- Privacy by Design ➔facilitates compliance
- Privacy by Default ➔plug & play compliance

➔legal requirement for PbD necessary

Approach


classical IT security protection goals
Integrity
Availability
Unlinkability
Transparency
Confidentiality
Intervenability
privacy-specific protection goals
Balancing needed!

Approach


Art. 6(d) dGDPR
classical IT security protection goals
Integrity
Balancing needed!
Art. 17 dGDPR
Art. 5, 6(b) dGDPR
Availability
Unlinkability
Art. 10 f. dGDPR
Art. 16, 17 dGDPR
Transparency
Confidentiality
privacy-specific protection goals
Art. 12(b-c), 14 (a-b) dGDPR
Intervenability

Section 5 LDSG SH

The controller and the processor shall implement the appropriate technical and organisational measures to ensure that processing operations (data, systems, processes)

- are available in a timely manner and can be used in accordance with this regulation (**availability**),
- remain intact, complete, accountable and up-to-date (**integrity**),
- can be accessed only by those authorized to have access (**confidentiality**).
- can be understood, reconstructed and evaluated with reasonable effort (**transparency**).
- prevent or allow only with disproportionate effort linking of personal data for a purpose other than the purpose stated at the time of collection (**un-linkability**), and
- that they are designed so that the data subjects can exercise the rights granted to them pursuant to this regulation and that they, controllers and data protection authorities can intervene in the data processing (**intervenability**),

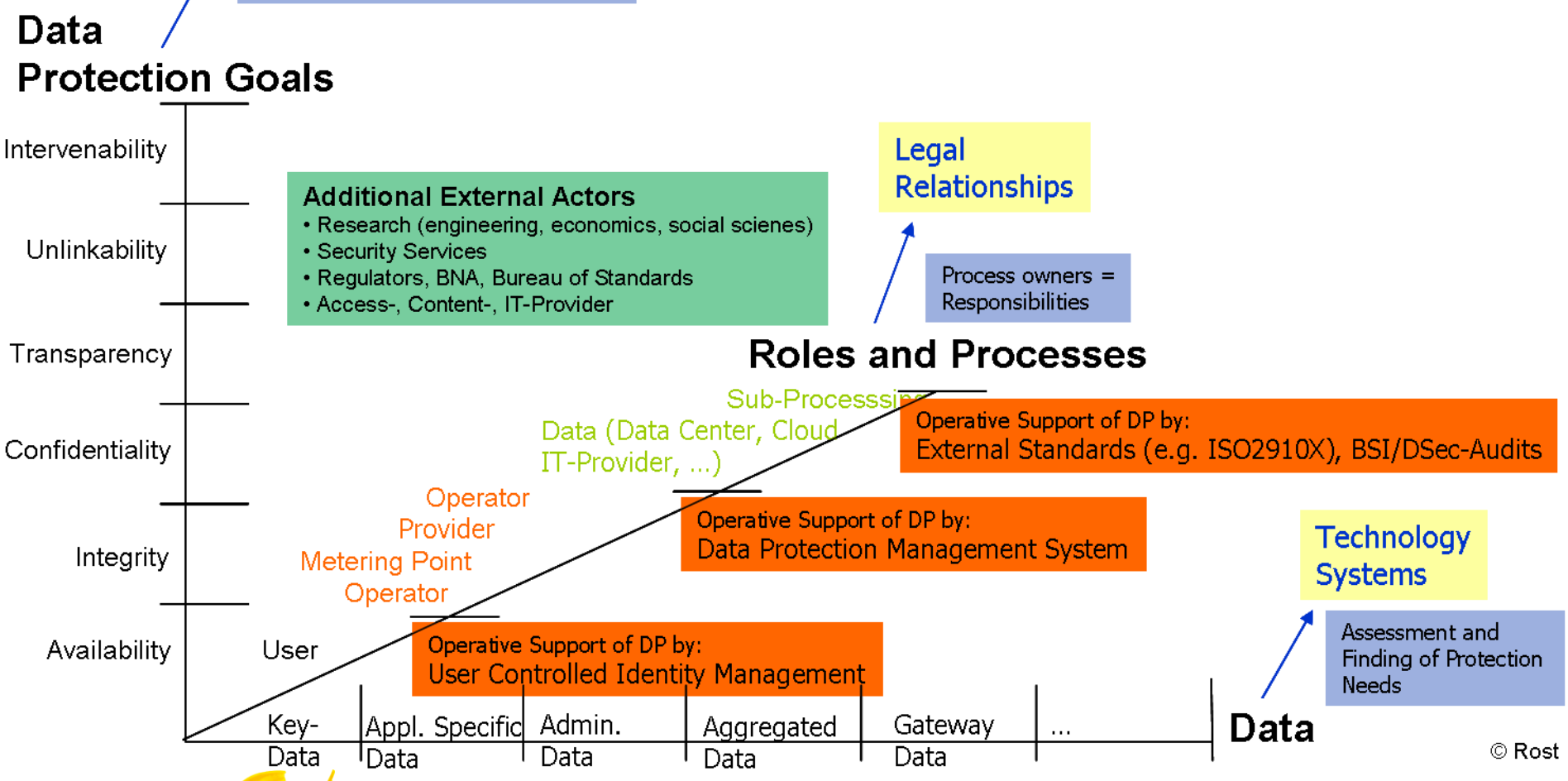
and be able to demonstrate the measures taken

Differentiated Risk Assessment for Technical-Organisational Measures

EuroPriSe European Privacy Seal

Protection Measures

1. Legal Balancing of Protection Goals
2. Protection Measures Catalogues



Standardizing Data Protection

Privacy by Design

Legislation

Protection Goals (6)

- Intervenability
- Unlinkability
- Transparency
- Confidentiality
- Integrity
- Availability

Process Components (3)
- Data
- Systems
- Procedures

Protection Demand / Risk Analysis (3)
- Normal
- High
- Very high

Reference Measures
- Documentation
- Management
- Audit
- …

From these building blocs a reference model of **54 specific data protection measures** can be derived!

Protection Measures in place
- Documentation
- Management
- Audit
- …

Each and every personal data processing can be subject to a generic and scalable assessment!

Thank You!

Contact:

kbock@datenschutzzentrum.de

www.european-privacy-seal.de

Standardizing Data Protection

Protection Goals (6)

- Intervenability
- Unlinkability
- Transparency
- Confidentiality
- Integrity
- Availability

Process Components (3)
- Data
- Systems
- Procedures

Protection Demand / Risk Analysis (3)
- Normal
- High
- Very high

From these building blocs a reference model of **54 specific data protection measures** can be derived!

Each and every personal data processing can be subject to a generic and scalable assessment!

DPGs Transport Normative Requirements