6th INTERNATIONAL CONFERENCE | 23 24 25 JANUARY 2013 | BRUSSELS BELGIUM
COMPUTERS, PRIVACY & DATA PROTECTION
RELOADING DATA PROTECTION
WWW.CPDPCONFERENCES.ORG

Privacy by Design with or without information security?

Kirsten Bock

CPDP 01-23-2013

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
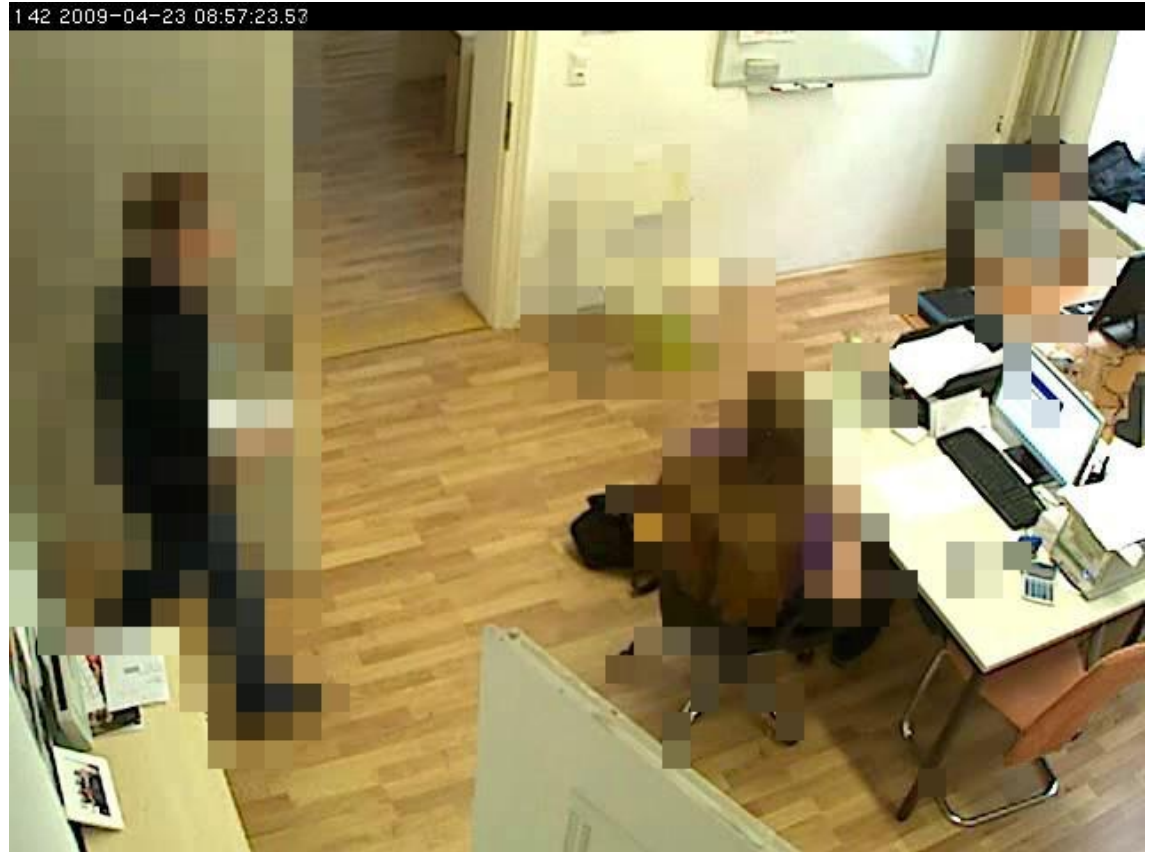➔ Privacy can be a market niche

Promoting PET solutions

Example:

KiwiVision (08/2009)

Privacy Protector,

Software module for integration in a video management system

Version 1.0

1 42 2009-04-23 08:57:23.53

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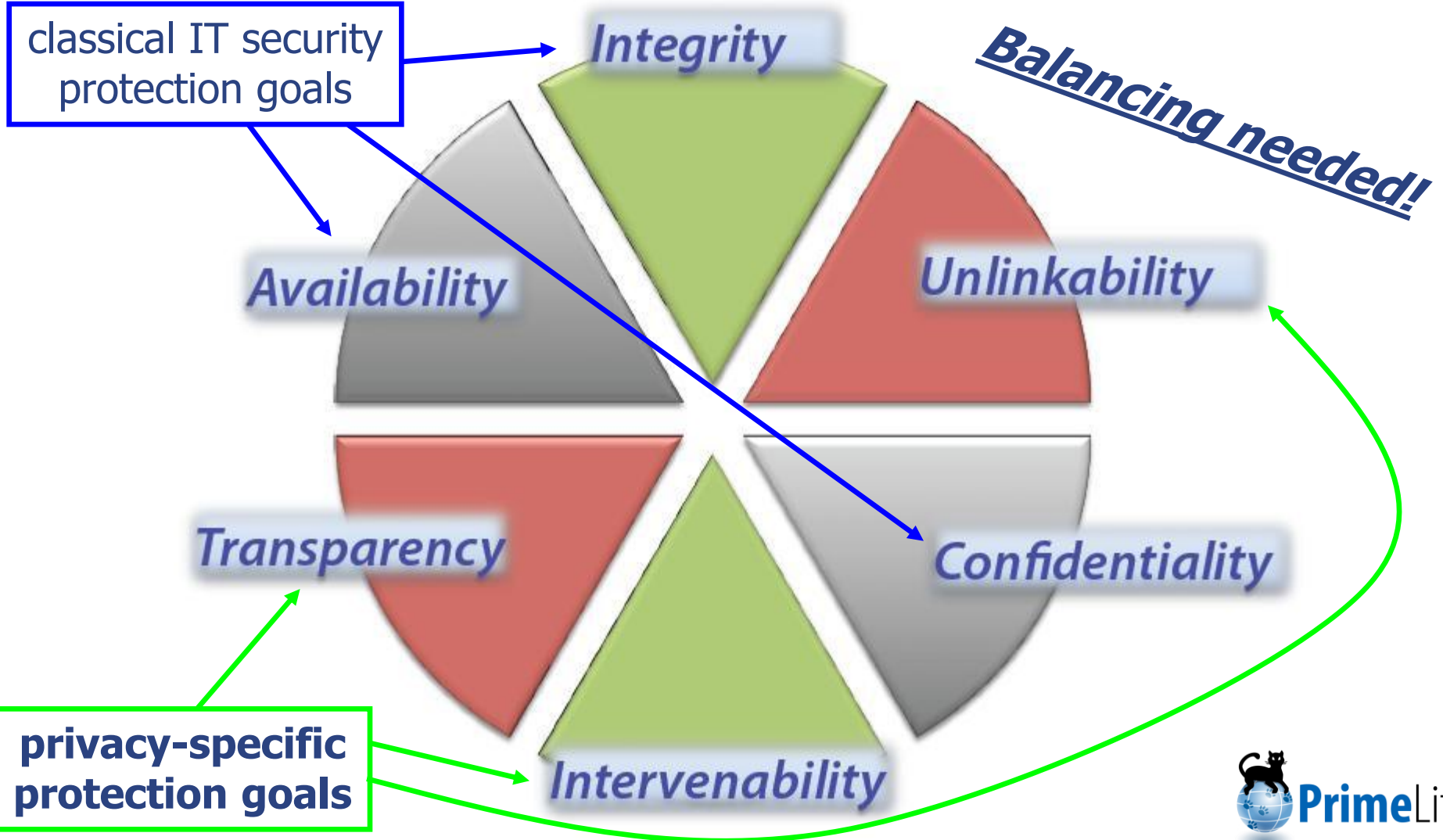
Privacy by Design

=

Managing the organisation of IT security

with respect to
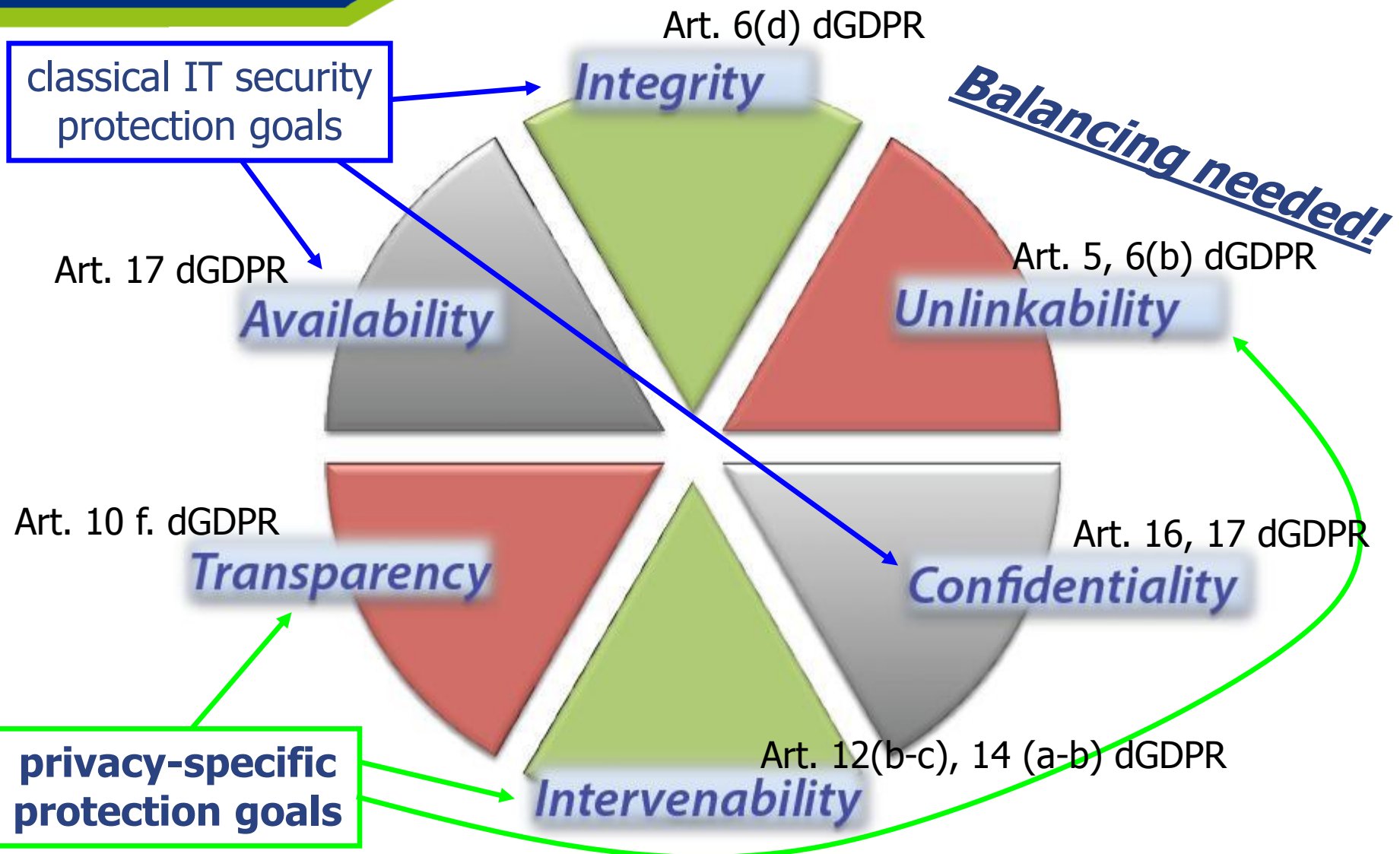
<u>safeguarding the fundamental right of

data protection</u>

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

classical IT security protection goals

Balancing needed!

Integrity

Availability

Unlinkability

Transparency

Confidentiality

Intervenability

privacy-specific protection goals

Art. 6(d) dGDPR

Integrity

Balancing needed!

classical IT security protection goals

Art. 5, 6(b) dGDPR

Unlinkability

Art. 17 dGDPR

Availability

Art. 16, 17 dGDPR

Confidentiality

Art. 10 f. dGDPR

Transparency

Art. 12(b-c), 14 (a-b) dGDPR

Intervenability

privacy-specific protection goals

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

EuroPriSe
European Privacy Seal

Protection Measures

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

Data Protection Goals

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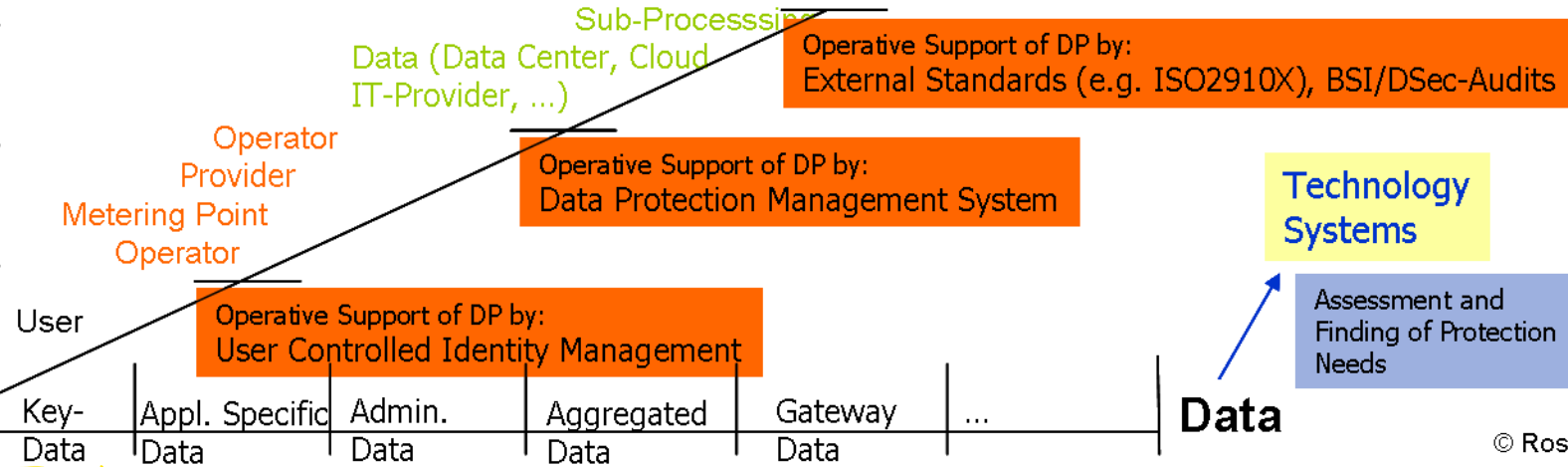- Transparency
- Confidentiality
- Integrity
- Availability

Additional External Actors
- Research (engineering, economics, social scienes)
- Security Services
- Regulators, BNA, Bureau of Standards
- Access-, Content-, IT-Provider

Legal Relationships

Process owners = Responsibilities

Roles and Processes

Sub-Processsing

Data (Data Center, Cloud IT-Provider, …)

Operator Provider Metering Point Operator

User

Operative Support of DP by: External Standards (e.g. ISO2910X), BSI/DSec-Audits

Operative Support of DP by: Data Protection Management System

Operative Support of DP by: User Controlled Identity Management

Technology Systems

Assessment and Finding of Protection Needs

| Key-Data | Appl. Specific Data | Admin. Data | Aggregated Data | Gateway Data | … | **Data** |

© Rost

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!

Data Protection

... is a basic human right

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

Art. 6(d) dGDPR

Integrity

•Accountability

Art. 5, 6(b) dGDPR

Unlinkability

•Purpose limitation

Art. 17 dGDPR

Availability

Art. 16, 17 dGDPR

Confidentiality

Art. 10 f. dGDPR

Transparency

•Right to information / Notice
•Documentation/procedure register
•Breach notification

Art. 12(b-c), 14 (a-b) dGDPR

Intervenability

•Data subject rights / Choice
•Data portability
•Reversibility+ correction