
PRIVACY-BY-DESIGN
Haute Couture or Ready to Wear
Dr. John J. Borking

That's me ≠ I am personal data

- **Dr. J. J. Borking * 1945 - Director /Owner Borking Consultancy Wassenaar Netherlands**
- **Of counsel Privacy-by-Design - Law firm CMS Derks Star Busmann in Utrecht**
- chairman Complaints and Disputes Committee eRecognition
- **EU/ CEN/ NR Researcher & Researcher e-Law University of Leiden**
- **Arbitrator/ Mediator SGOA (ADR- ICT)**
- **Former Privacy Commissioner & Board Member Dutch Data Protection Authority**
- **Senior Counsel Europe Xerox Corp**

MENU

- What is Privacy-by-Design?
- Legal specifications for privacy knowledge engineering
- How to build DP principles to be applied in the design of communication and information systems
- PbD haute Couture and Ready to wear
- Adoption factors for PbD
- Conclusions

PRISM WikiLeaks?

VideoClip Ennemy of the State 1998

The Surveillance State

- **Michel Foucault,** "History of Systems of Thought" addresses the concept of power, how it works, the manner in which it controls knowledge v.v. and how it is used as a form of social **control**.(Panopticon)
- Society has become a risk control / surveillance state, organized and structured with surveillance techniques enabled by ICT (J.Borking, 2010, p.83)
- What could be the consequences for:
  - Identity management?
  - Privacy?
- How to protect ourselves? ICT services should be designed to maintain privacy (N.Gilbert, 2007)

UNDERSTANDING

- The Cholera metaphor
- The law alone can't protect privacy (not self- executing; more than 90 % violations)
- From reactive to proactive bridging the data protection law and ICT technology- (SWOT1994 DPA Netherlands; Van Rossum H. et all, 1995)
- Constructing I.S. that protect privacy & IT services that maintain privacy i.e. building the law into the I.S.

History of PETs/PbD 1995-2013

- Joint paper 1995 TNO FEL, RGK and IPC Toronto taking a generic look at privacy from a designer ‘s perspective: PET + design patterns/architecture
- First time use of the term PbD 2000 conference Computers, Freedom and Privacy
- First time applied PbD design in EU FP 5 PISA project 2000-2003
- Promoting PbD since 2009 Ann Cavoukian
- Draft GDPR 2012 article 23

WHAT IS PRIVACY BY DESIGN? 1

- Article 23 of the Draft GDPR requires “data protection by design” and “data protection by default”. (DPbD is applauded as a core innovation of reform (Albrecht Report 2012/011 (COD))
- Privacy or Data protection or Compliance by Design ?
- Having regard to the state of art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
- The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

WHAT IS PRIVACY BY DESIGN? 2

Article 23: linguistic elements: “data protection” and “design” connected with the word ‘*by*’. Design is described as: “*to create, execute, or to have as a purpose, to devise for a specific function or end, or to make a drawing, pattern, or sketch*. The word: ‘*by*’ implies that data protection purposely has to be realized by design

Websters Third New International Dictionary (a Meriam Webster), Chicago p.611-612

WHAT IS PRIVACY BY DESIGN 3

The objective is:

1. Privacy assurance must ideally become an organization's default mode of operation (…) by deploying PETs (…) extending to a trilogy of encompassing applications: 1. IT systems; 2. Accountable business practices; 3.Physical design and networked infrastructure. (IPC Ontario 2009)

2.The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), privacy by default settings and the necessary tools to enable users to better protect their personal data (e.g. access controls, encryption). (WP 168 The Future of Privacy p.13)

- 3.The principle of Privacy by design means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. (COM (2010) 245)
- 4.Also for creating transparency and opacity concerning the processing of personal data (Borking, 2010, p.191)

WHAT IS PRIVACY BY DESIGN? 4

DESIGN
GUIDED BY
PRIVACY
PRINCIPLES
AND VALUES

INFORMATION TECHNOLOGY
PRIVACY SUPPORTING
ARCHITECTURE
PRIVACY ENHANCING
TECHNOLOGIES

ORGANIZATION

PRIVACY SUPPORTING BUSINESSES
& PROCESSES & PIAs
MANAGEMENT SUPPORT FOR
PRIVACY

PHYSICAL ENVIRONMENT
PRIVACY SUPPORTING ORGANIZ-
ATION OF PHYSICAL SPACES

EXPERIENCE
OF PRIVACY,
ESSENTIAL
FOR PRIVACY,
TRUST AND
ADOPTION

M. Van Lieshout
Stimulerende en
remmende factoren van
Privacy -by -Design in
Nederland (2012)

What is Privacy-by-Design? 5

- Article 23 paragraph 1 : ten amendments and article23 paragraph 2 : twelve amendments. *"Data protection by design is applauded as a core innovation of the reform. This would ensure that only data that are necessary for a specific purpose will actually be processed."*
- Albrecht, 2012, p. 176;
- Total amendments approx, 4000

Privacy-by-Design avant la lettre

RECITAL 46 & ARTICLE 17 - 95/46/EC

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly (…) to prevent any unauthorized processing;

(17) The person responsible shall take suitable technical and organizational measures to protect personal data both at the design & processing phase of the system: Against loss, Against any form of unlawfull processing,To prevent unnecessary collection and further processing Considering state of art, costs, risks

(such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected)

LEGAL SPECs (PRIME)

PRINCIPLES CONCERNING THE FUNDAMENTAL DESIGN OF APPLICATIONS:

1 Data minimization (maximum anonymity and early erasure of data)

2 Transparency of processing

3 Security (security specs from privacy threat/ risk/ vulnerability analysis)

PRINCIPLES CONCERNING THE LAWFULNESS OF PROCESSING:

1 Legality (e.g. consent)

2 Special categories of personal data

3 Finality and purpose limitation

4 Data quality

PRINCIPLES CONCERNING THE RIGHTS OF THE DATA SUBJECT:

1 Information requirements = Notification requirements

2 Access, correction, erasure, blocking

3 Objection to processing

4 Confidentiality / data traffic / location data / spam

PRINCIPLES CONCERNING DATA TRAFFIC WITH THIRD COUNTRIES

PRINCIPLES CONCERNING PROCESSING BY A PROCESSOR RESPONSIBILITY AND CONTROL

ONE EXAMPLE OF PbD 1:
The Identity Protector

USER KNOWN

THE IDENTITY PROTECTOR

PID 1

PID 2

PID n

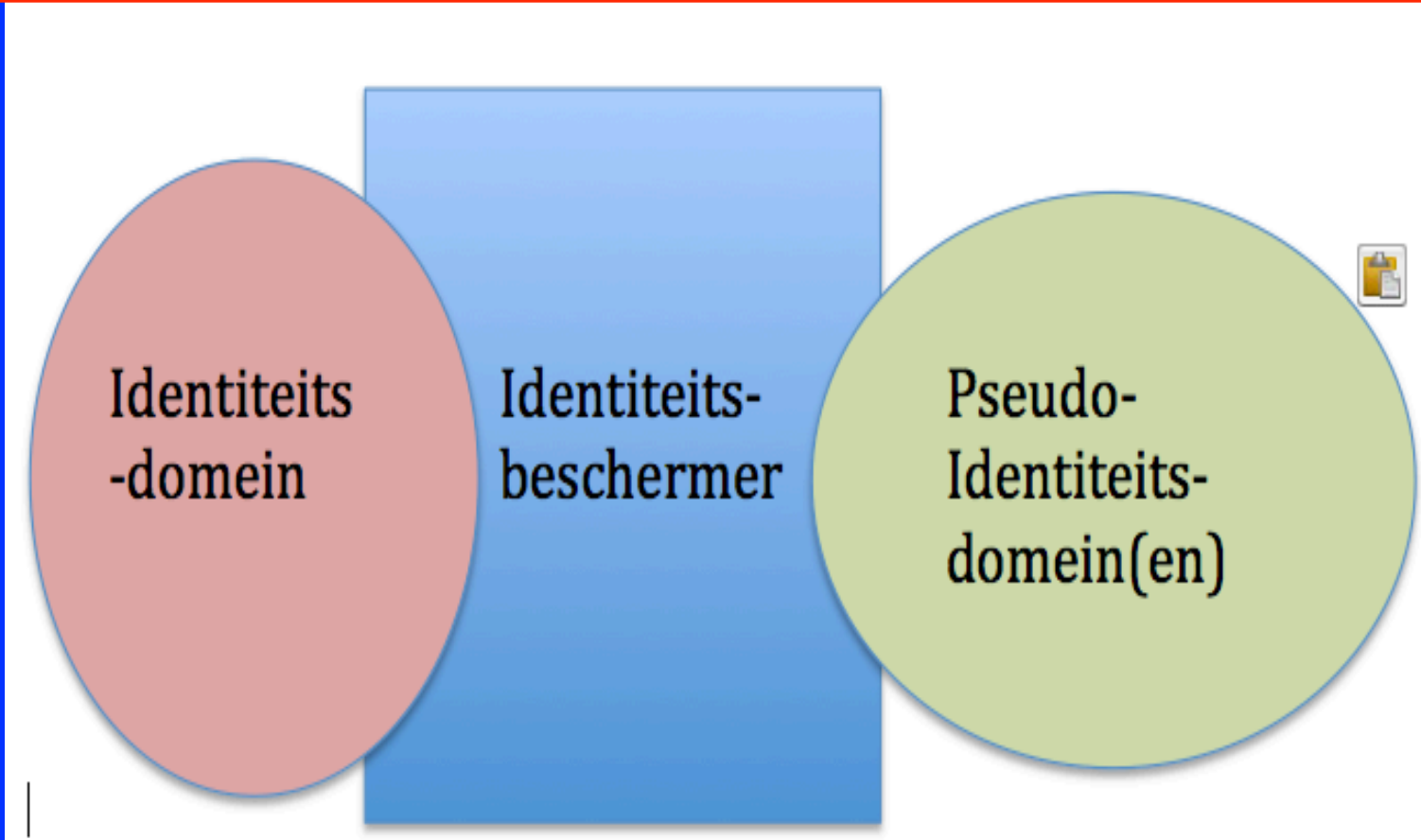
IDENTITY DOMAIN

Borking J., Der Identity-Protector, *Datenschutz und Datensicherheit (DuD)* 1996, 11

PSEUDO IDENTITY DOMAIN

ONE EXAMPLE OF PbD 2

SEPARATION OF DOMAINS



Koorn R., et all, Privacy Enhancing Technologies, Witboek voor Beslissers,, Den Haag, 2004

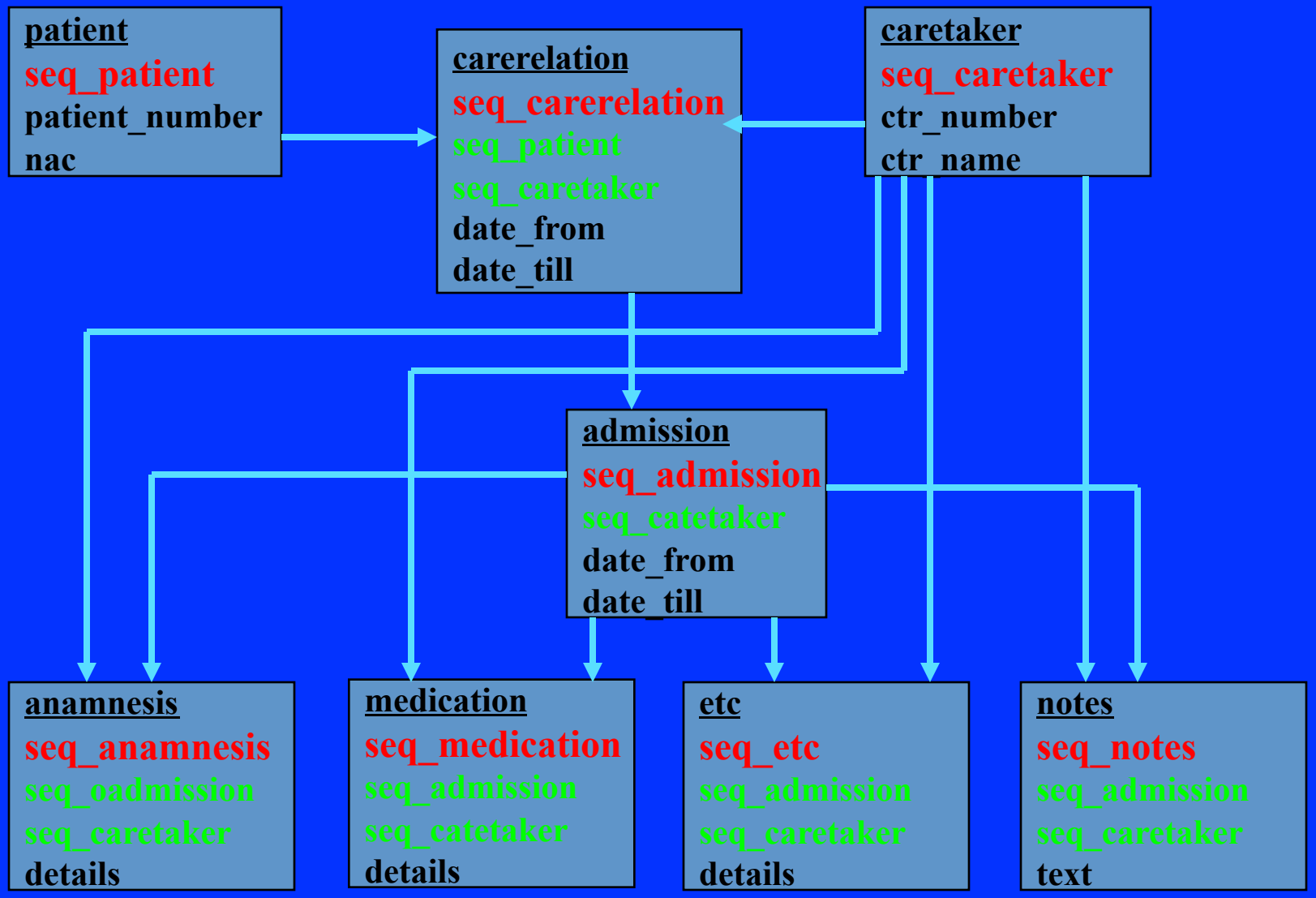
THE WORKINGS OF THE IDP

An identity protector performs the following functions:

- It generates pseudo-identities as needed;
- It converts pseudo-identities into actual identities (as desired)
- It combats fraud and misuse of the system
- At least two domains are created: an *identity* domain and a *pseudo* domain, one in which the user's actual identity is known and accessible, and one in which it is not.
- It permits the designer of a system to minimize the collection of personal data stored in the database

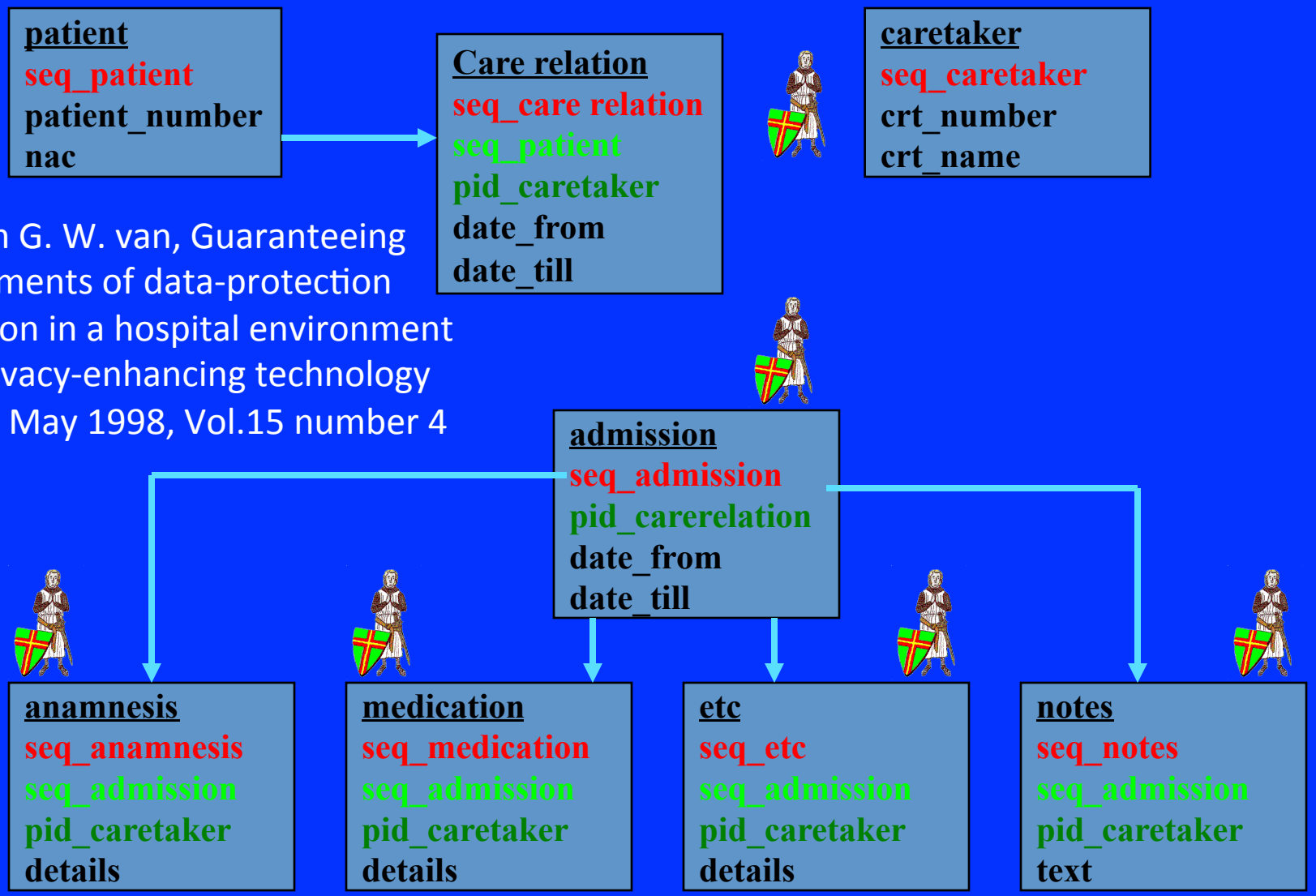
Hes R. & J.Borking, Privacy Enhancing Technologies: The Path to Anonymity, The Hague 2000 , www.cbpweb.nl

Hospital Information System with Basic tables with relational links in RDB



ONE PRACTICAL EXAMPLE OF PbD: Hospital Information System

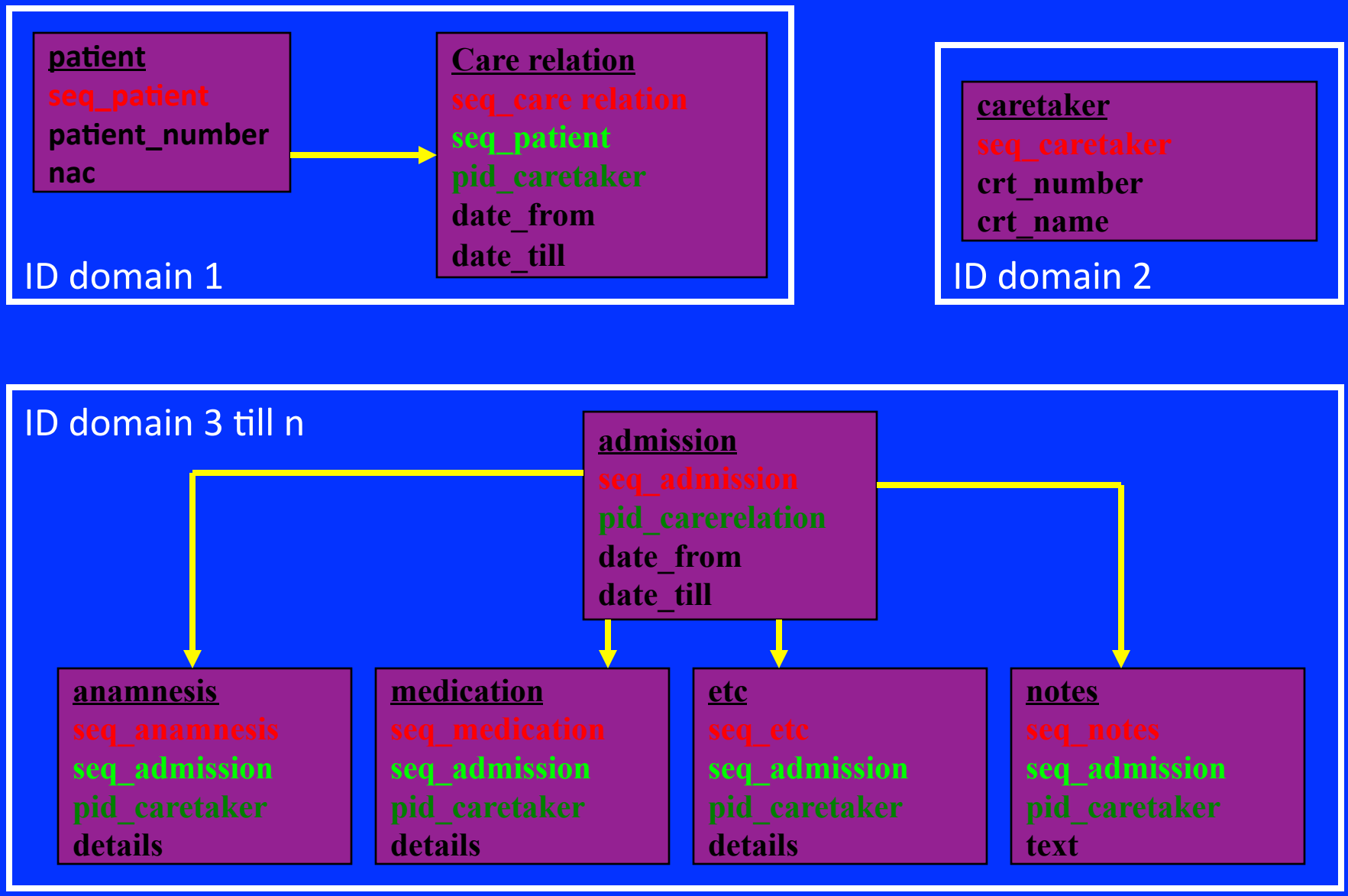
Hospital Information System Basic tables with Pseudo Identities & ID Domains



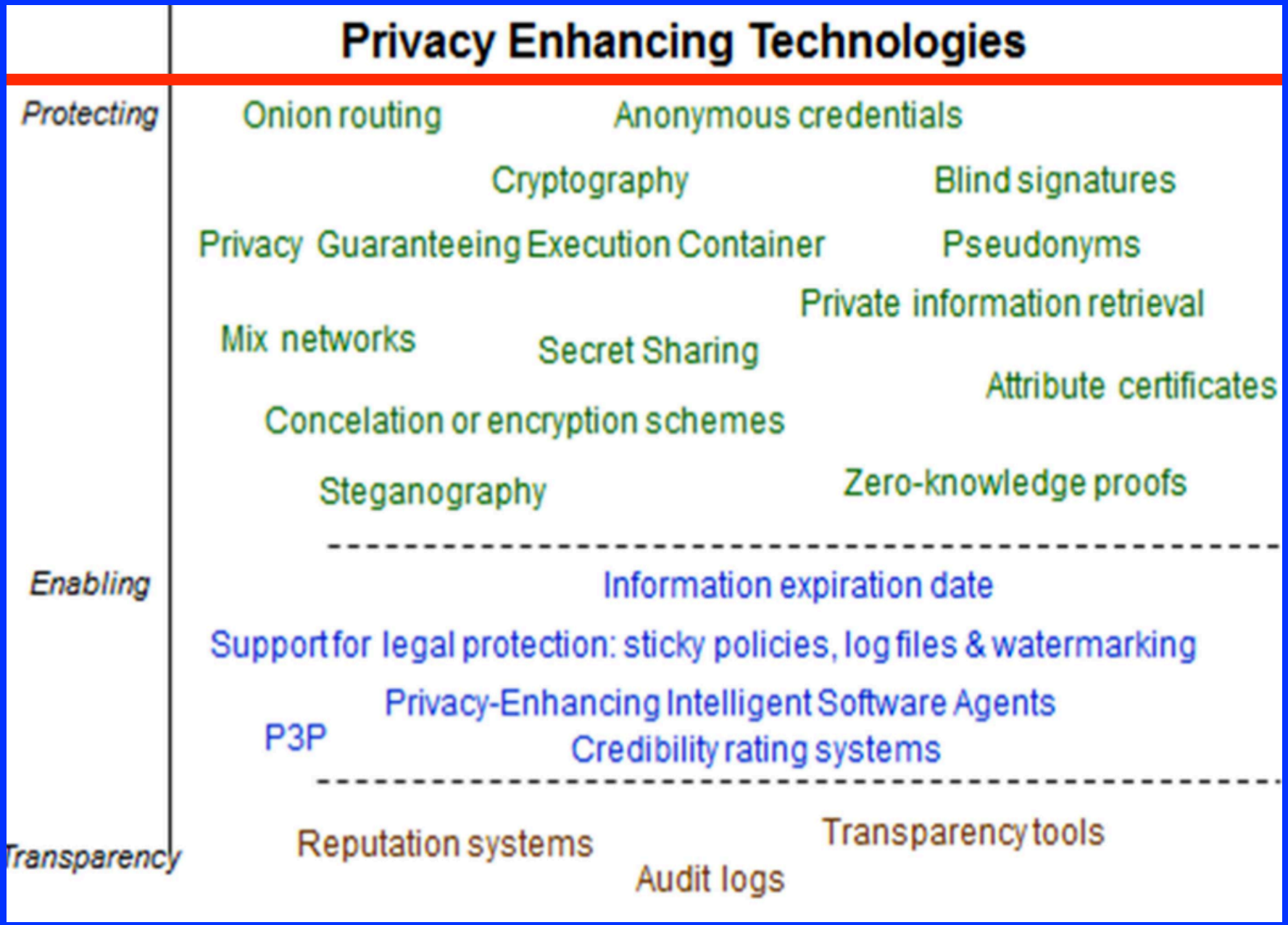
Blarkom G. W. van, Guaranteeing requirements of data-protection legislation in a hospital environment with privacy-enhancing technology *BJHCIM* May 1998, Vol.15 number 4

HOSPITAL INFORMATION SYSTEM

ID Domain 3 till n for research purposes



Privacy Enhancing Technologies



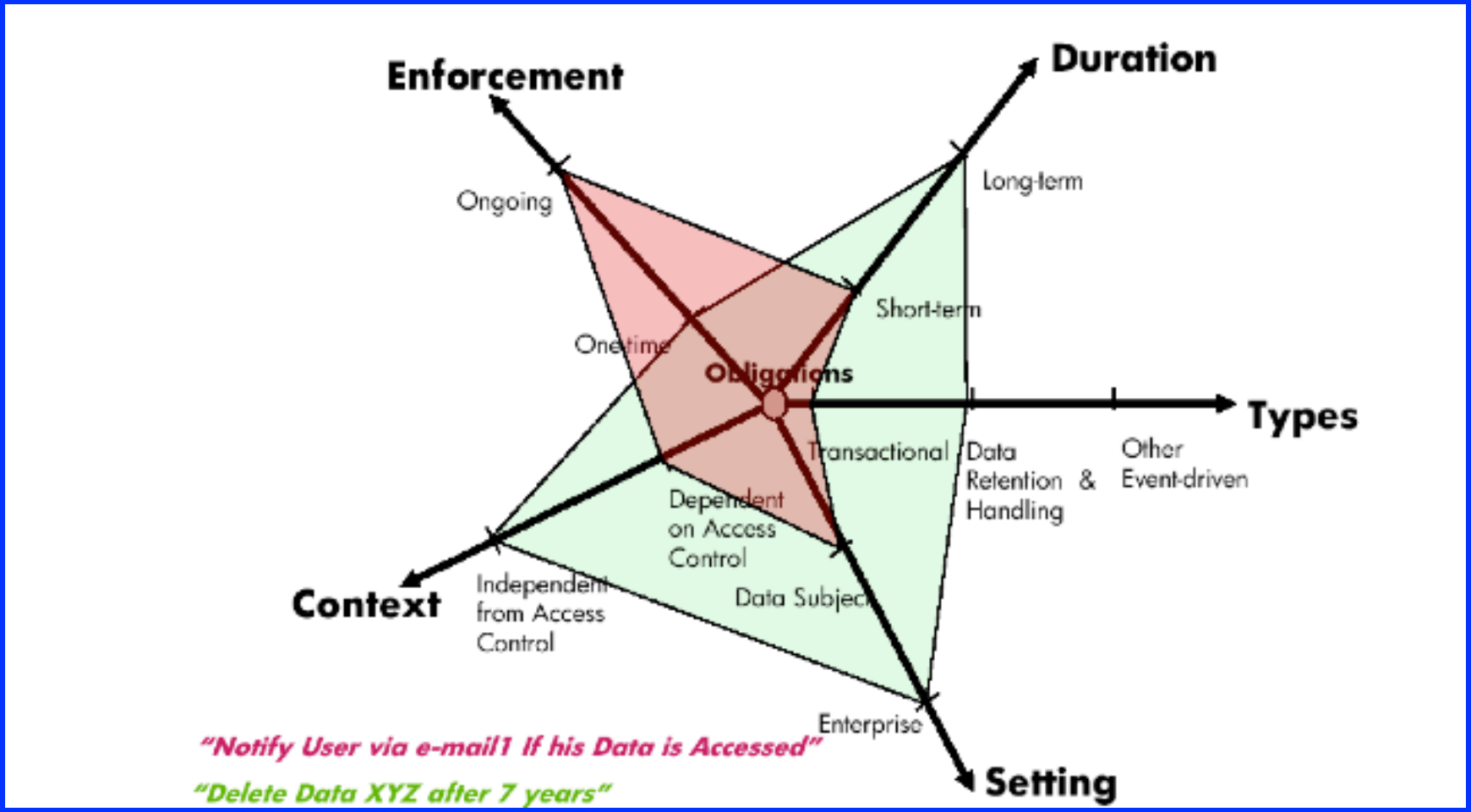
PIA SINE QUA NON FOR PbD

- Without a methodology (a systematic process) for assessing the threats, vulnerabilities and impact on privacy of a project, policy, program, service, product or other initiative that involves the processing of personal information , it will be impossible to execute PbD in a proper way. (cfr. Art. 33 GDPR)
- Five key stages in the PIA report : A. Project / Service description; B. Mapping the information flows and privacy framework; C. Privacy impact analysis; D. Privacy management; E. Recommendations: Produce a final PIA report covering the above stages including recommendations.

How to build DP principles to be applied in the design of communication and information systems

- PbD Haute couture e.g. *Obligation Management System* (OMS) (Cassassa Mont, 2006) & privacy ontologies
- PbD 'ready to wear'
- PbD building principles analogous to Object Oriented Software Design
- What If Encryption Isn't An Option?
- Privacy management systems rule based

PRIVACY BY DESIGN HAUT COUTURE



Cassassa Mont 2006

PRIVACY ONTOLOGIES FOR PMS 2003 – 2008 - 2011

Definition:

Formal machine understandable description of terms and relations in a particular domain (Bench-Capon 2007)

For privacy protection:

Encapsulation of knowledge about the data protection domain and relationships between concepts in an unambiguous standardization and legal instantiation

HCI: 4 Cs: Comprehension = to know, to understand, Consciousness =to be aware, informed, Control = to manipulate, to be empowered, Consent= to agree

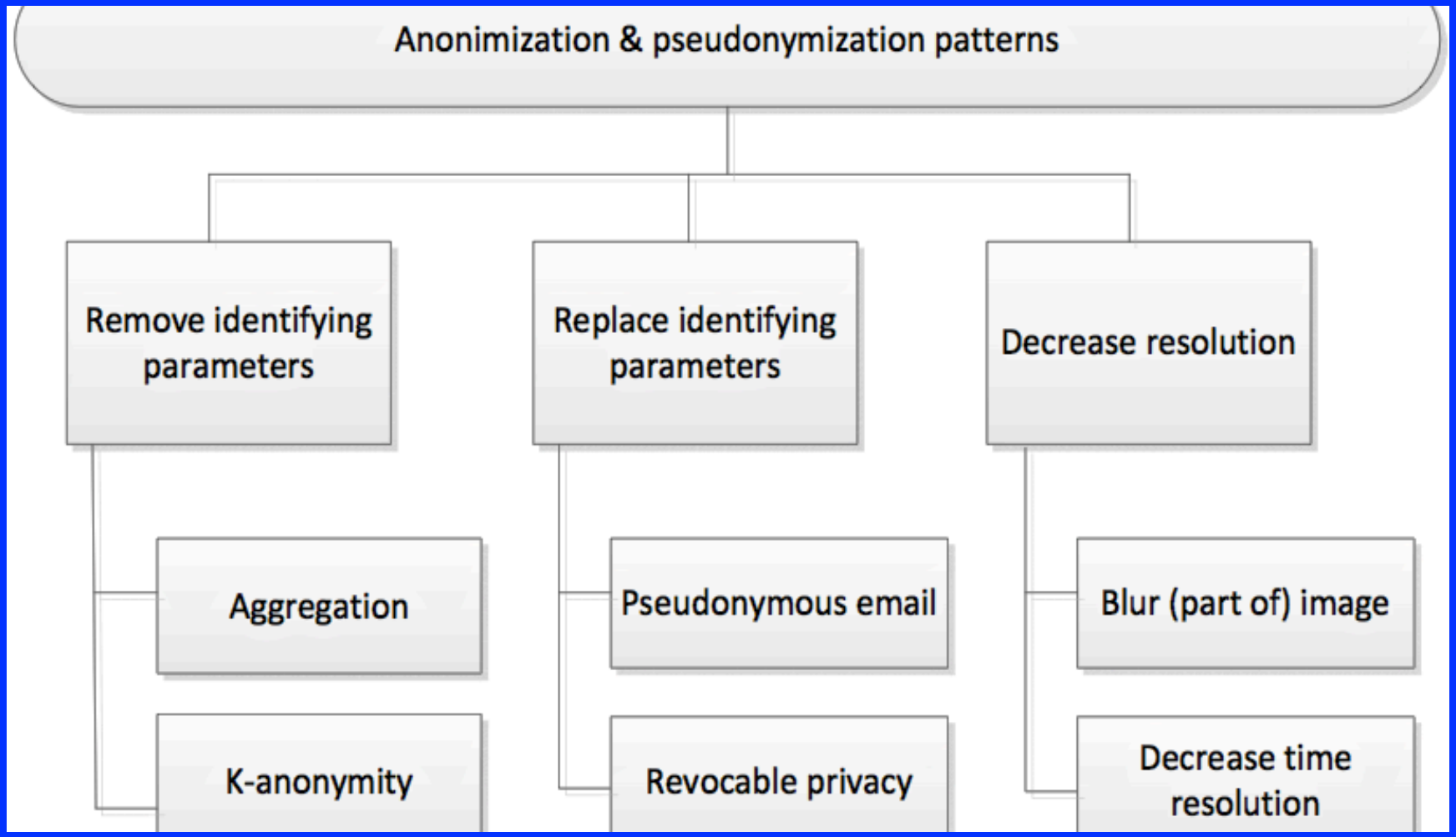
Camenish J., R.Leenes & D. Sommer, PRIME, Brussels, 2008

PbD BUILDING PRINCIPLES
Object Oriented privacy knowledge engineering, the use of patterns

Privacy Risk Management and selection of building patterns for: (not limited to)

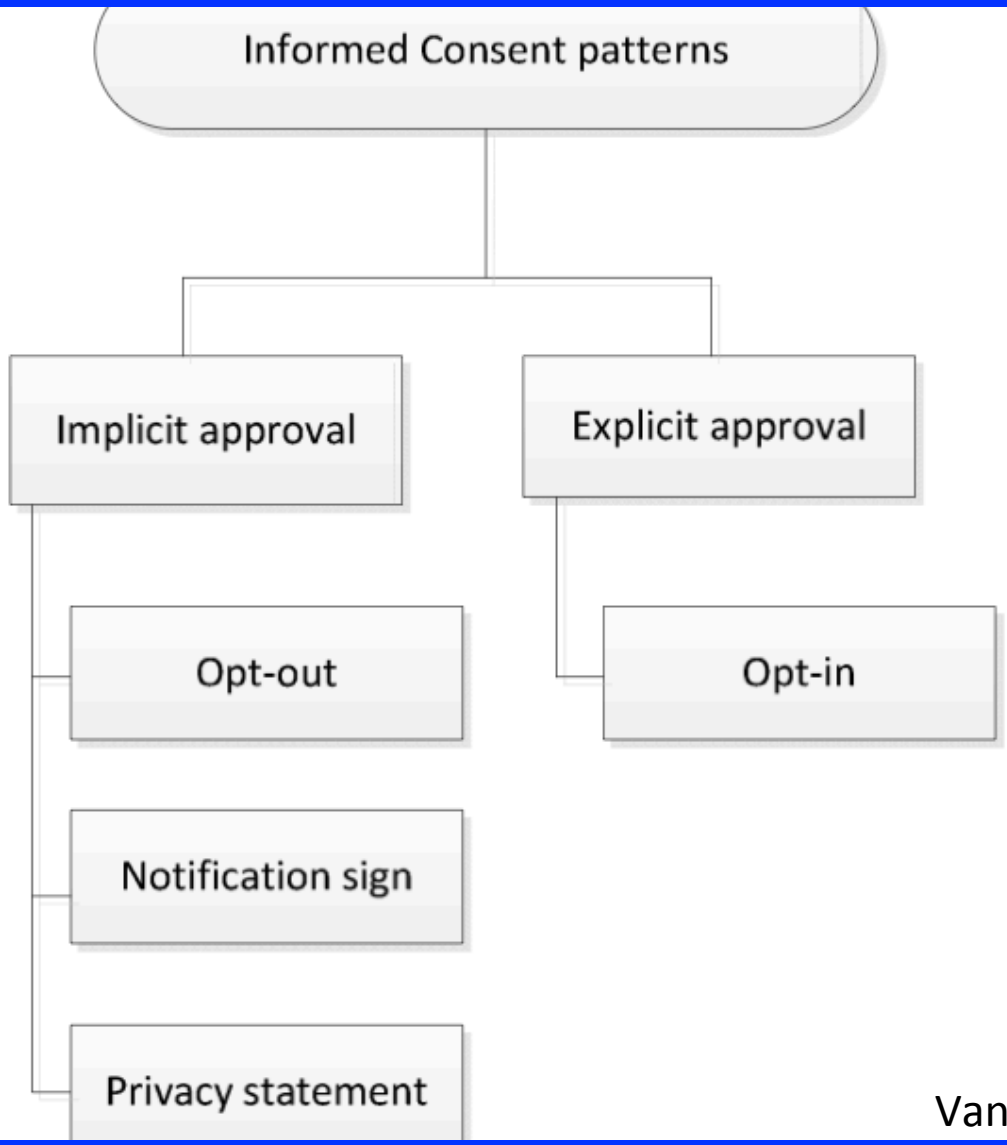
- Privacy requirements patterns
- Anonimization and pseudonymization
- Hiding of personal data
- Data minimization
- Transparency
- Auditing and accounting
- Informed consent (Van Rest, 2012)

PRIVACY BY DESIGN READY TO WEAR PATTERNS 1



Van Rest 2012

PRIVACY BY DESIGN READY TO WEAR PATTERNS 2



Van Rest 2012

What If Encryption Isn't An Option?

- Privacy management systems rule based (PISA 2003- Zero Knowledge Systems)
- Key privacy parameters: **1.actors, 2.data, 3.actions, 4.purpose and 5.conditions**. Using these parameters an organization can model and design their privacy practise (policy and data handling processes). For example consent can be modelled with a Condition parameter.
- For example, ABC Bank [actor] may disclose [action] customer phone number [data] to ABC Marketing Department [actor] for offering new services [purpose] if customer has consented to ABC Bank offering new service by telephone [condition].
-

PROBLEMS FOR PRIVACY BY DESIGN

- PbD is done mostly without a proper privacy risk analysis up front (PIA) (Borking, 2010)
- The translation of PbD (the legal specs) into actual designs of systems is done by example. Therefore, everybody is free to postulate a particular design (process) as "Privacy or Data Protection by Design" (Van Rest, 2012)
- On top of that, actual implementation of PbD is confronted with difficulties such as lack of economic incentives, transparency of systems, legacy systems, and lack of **adoption** by organizations/end-users and consumers (Borking, 2010)

HOW FURTHER?

- Do we let each designing party (industry and government) decide per case or product line what PbD means (an evolutionary approach? Each different party implements PbD in its own way), or
- As we don't know enough of and cannot leave it to (behavioral) economics, that urgently justifies the need for EU Commission/ government/ DPA involvement
- Therefore: "to adopt delegated acts (…) for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2 (of article 23 GDPR), in particular for data protection by design requirements applicable across sectors, products and services.
- The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2.)

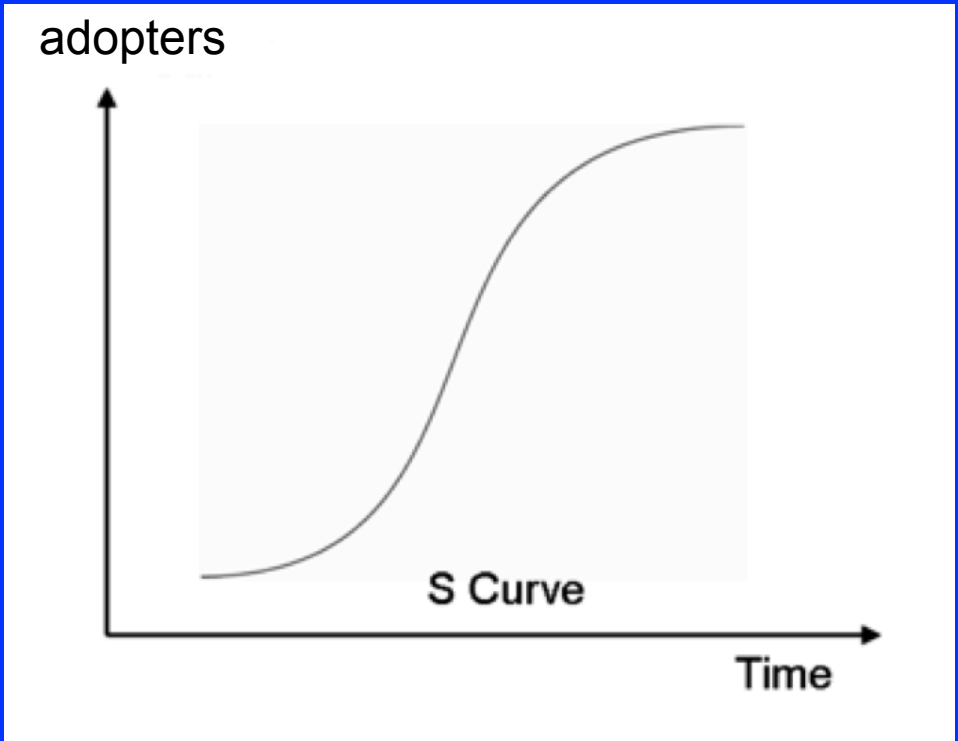
Organizational Adoption of PbD

- Central question:

  What are the Drivers and Inhibitors for adoption by organizations of PbD

  Research into the adoption of PETs
  (Borking, 2010 p. 305-341)

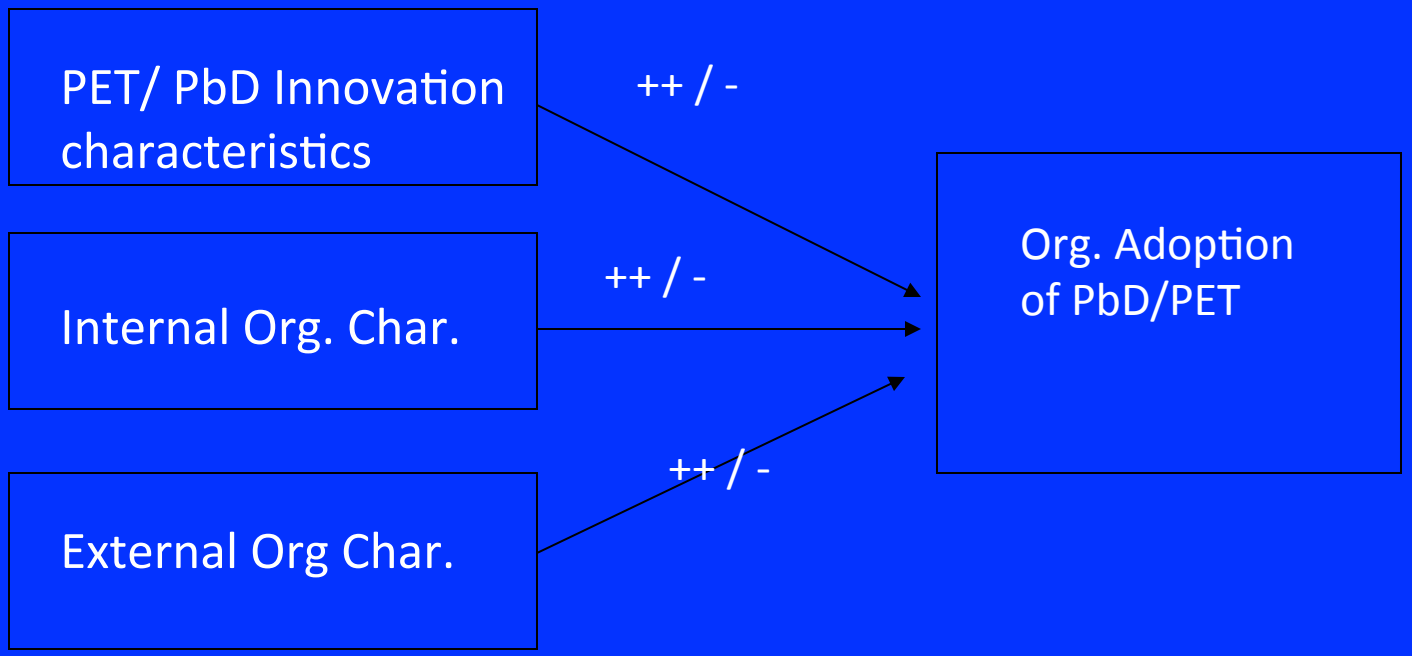
ROGER'S THEORIE ON THE DIFFUSION OF INNOVATIONS



Rogers, 2003, p.11

Literature Review

Studies by a.o. Rogers (2003) and Fichman (2000): Clusters of factors impacting adoption of IT based innovations.



Adoption factors 1

Positive:

- Relative Benefit
- Role of advisory institutions (like DPA)

Negative:

- Costs
- Compatibility
- Complexity
- PET woven into business processes

Adoption factors 2

Factor II: Internal Organizational Characteristics

Positive

- Perception and level of awareness of privacy regulation
- Type of Data processed (e.g. risks incurred)
- Individual Ties with advisory institutes
- Presence of Key persons

Negative

- Complexity of organizational processes
- Structure and size of the organization
- Diversity in Information Systems

Adoption factors 3

Factor III: External Organizational Characteristics

Positive

- Pressure by privacy legislation and DPAs
- Existing offer of PbD solutions

Negative

- Complexity of privacy law
- Private versus Public organizations

Adoption Conclusion

- Adoption of PbD/PET is problematic
- What helps is pressure on regulatory and legal compliance & information and advice on PbD/PET
  (Enforcement of Article 23 GDPR)
- Promoting role of the DPAs highly necessary (Ribbers 2007, p.20; Borking 2010 p.326)
- Perceived relative advantage of PbD seems minimal (Knowledge gap) Incentive: Article 79 GDPR: Administrative fine
- Also in Privacy laws insufficient reference to PbD yet. GDPR will change this

Measuring readiness for PbD by level of Identity and Access Management (IAM)

- ‘Identity and Access Management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources’ (Baladi, 2006)

PRIVACY MATURITY MODEL

- *"a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached."*

- Existing models: CMMi (SE Carnegie Mellon), Nolan Norton, INK (EFQM)….

IAM TOPOLOGY RE ORGANISATIONAL SEGMENTATION CONCERNING MATURITY

Authentication Management	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Authentication Requirements based on a one time survey	Authentication Requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continously adjusted
User Management	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorization sources, automated procedures
Authorisation Management	No authorization matrixes, authorization is defined ad hoc	Authorization matrixes defined but are not updated	Authorization matrixes are updated periodically	Role Based Access Control used for critical applications	Role Based Access Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited Automated unreliable processed locally	Limited Automated but reliable processes locally	Limited Automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No responsibility delegated into a AO/IC organization	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibility to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	**Starting-up**	**Active**	**Pro-Active**	**Top Class**

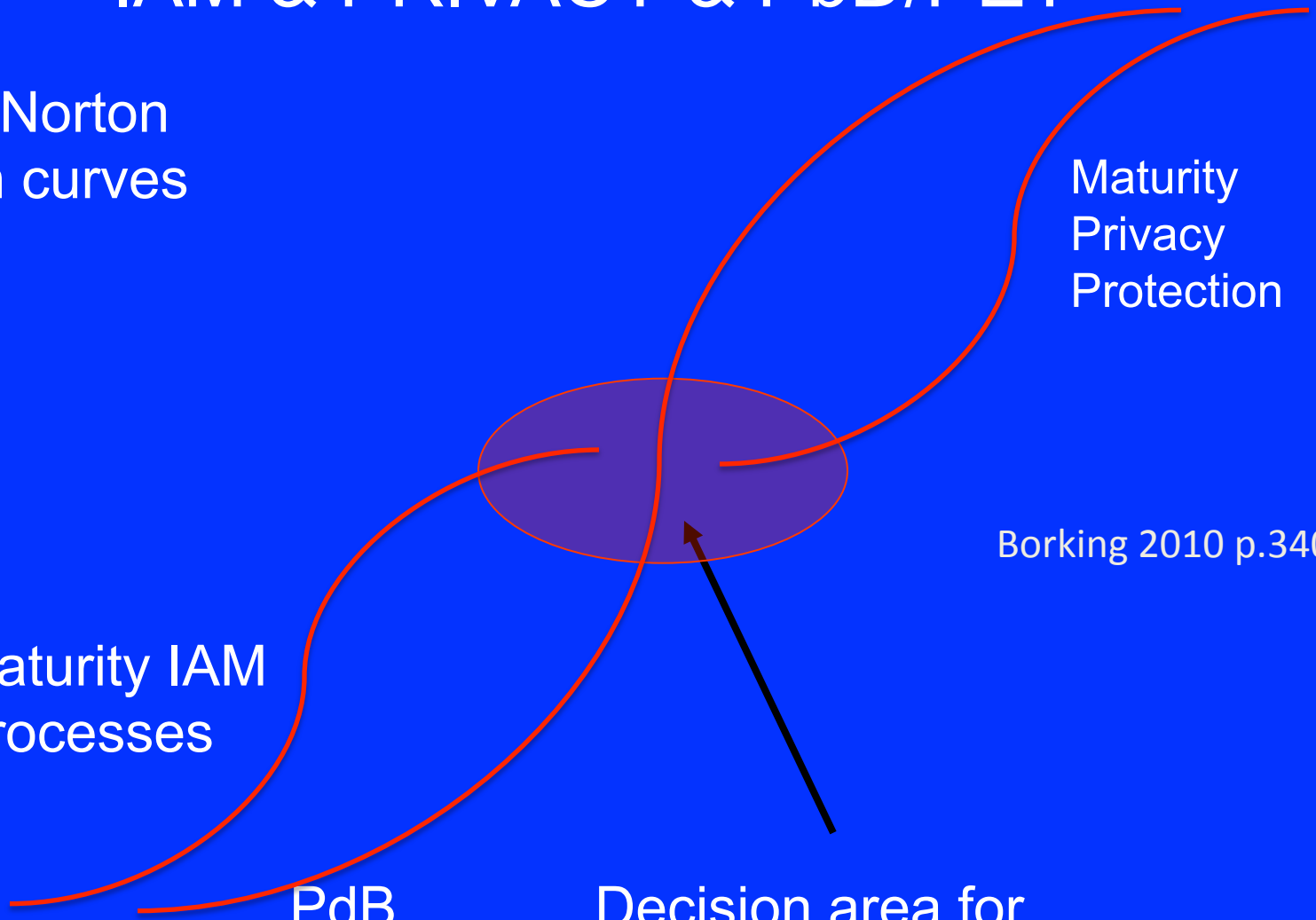
PRIVACY MATURITY

Initial	Activities are ad hoc, with: • No defined policies, rules, or procedures. • Eventually lower-level activities, not coordinated. • Redundancies and lack of teamwork and commitment.
Repeatable	The privacy policy is defined, with: • Some senior management commitment. • General awareness and commitment. • Specific plans in high-risk areas.
Defined	The privacy policy and organization are in place, with: • Risk assessments performed. • Priorities established and resources allocated accordingly. • Activities to coordinate and deploy effective privacy controls.
Managed	A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with: • Early consideration of privacy in systems and process development. • Privacy integrated in functions and performance objectives. • Monitoring on an organizational and functional level. • Periodic risk-based reviews.
Optimizing	Continual improvement of privacy policies, practices, and controls, with: • Changes systematically scrutinized for privacy impact. • Dedicated resources allocated to achieve privacy objectives. • A high level of cross-functional integration and teamwork to meet privacy objectives.

GAP Institute of Internal Auditors — *Source: Hargraves et al 2003*

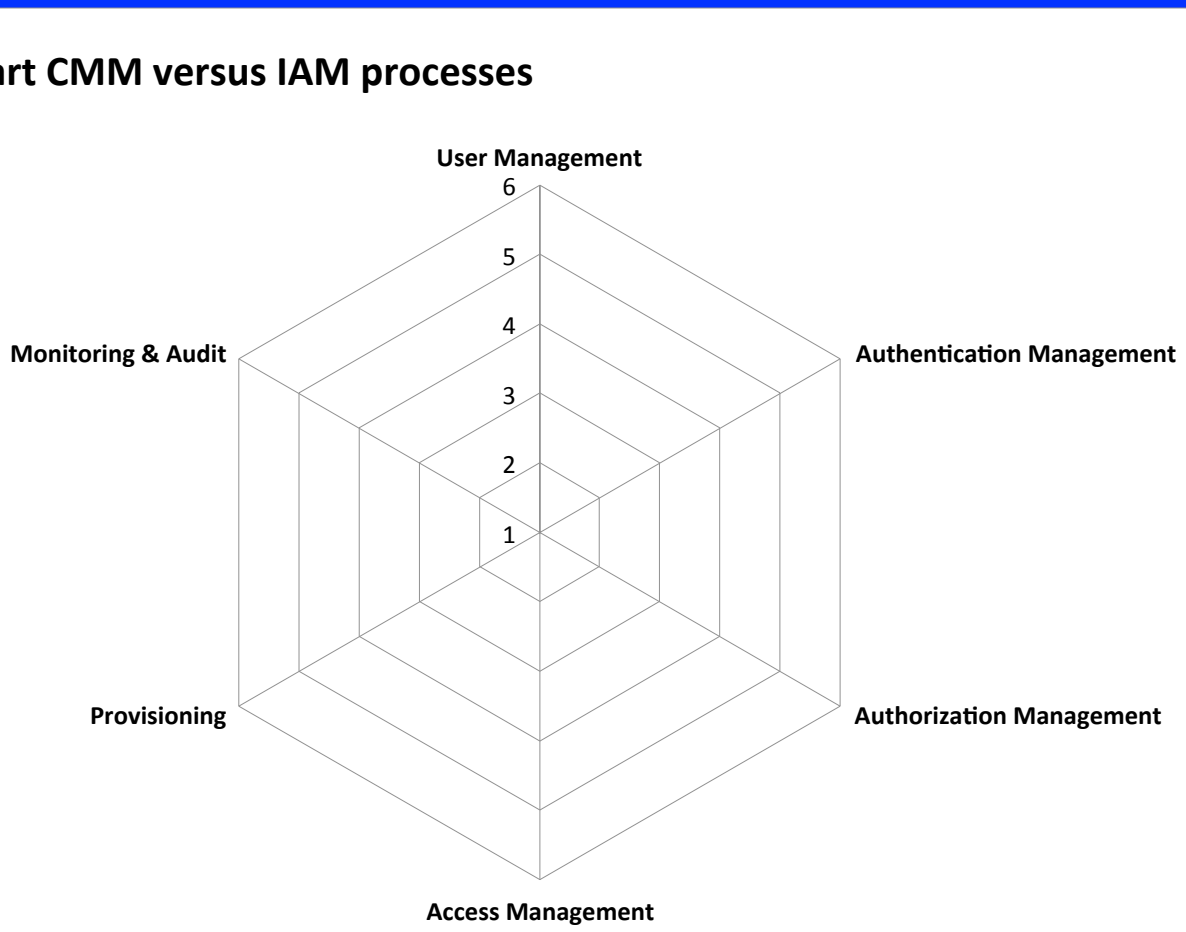
S- CURVES MATURITY IAM & PRIVACY & PbD/PET

Nolan Norton growth curves

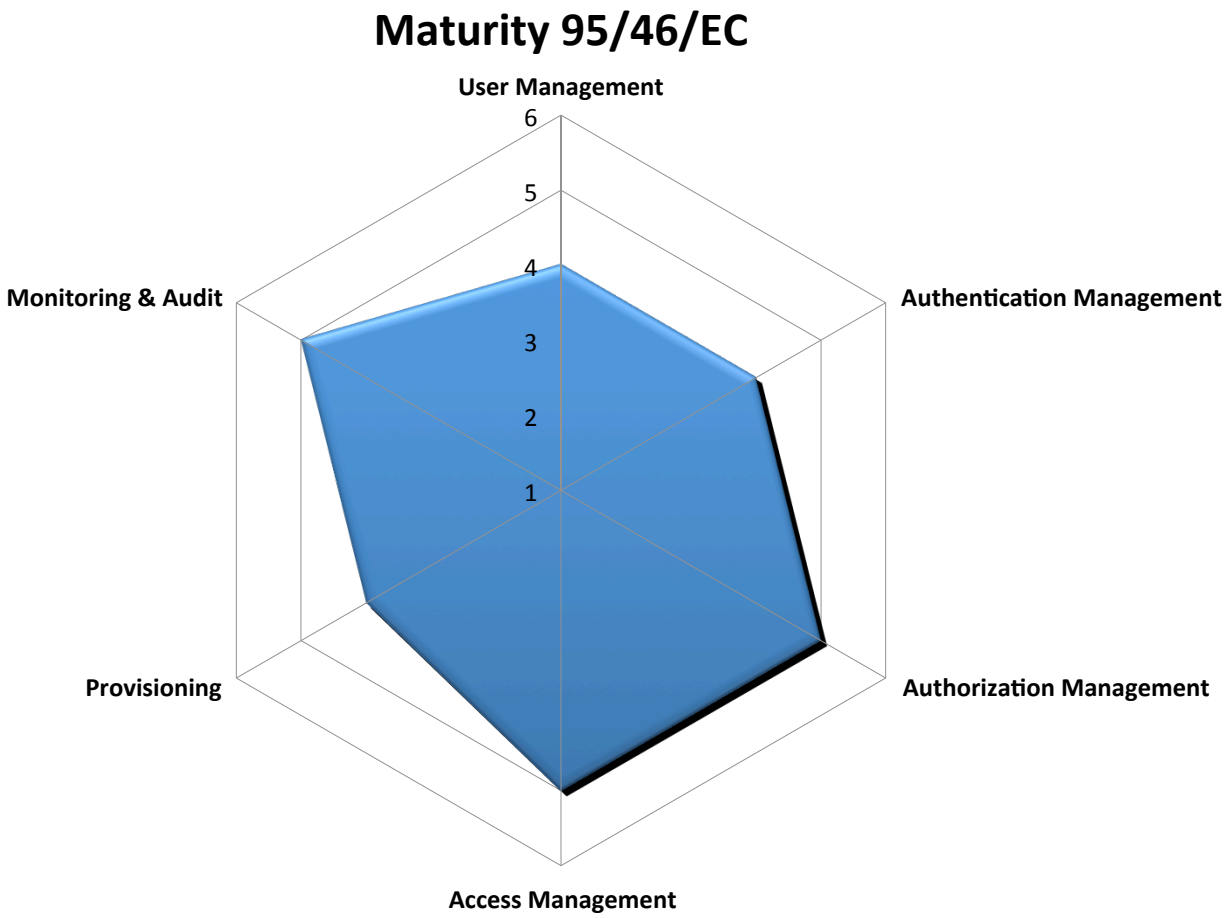


SPIDER CHART CCM* vs IAM

*Capability Maturity Model



95/46/EC GAUGING

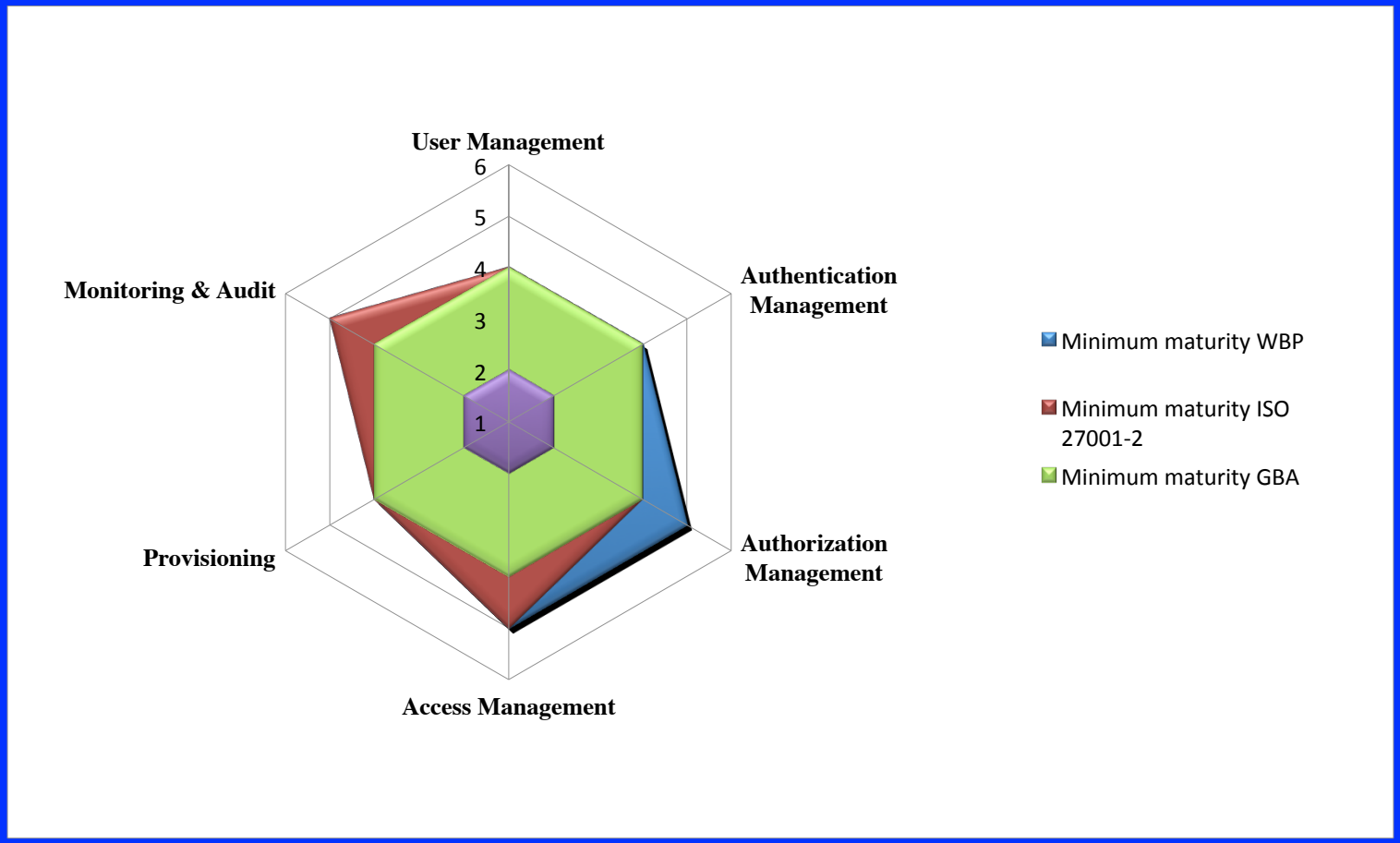


REQUIREMENTS

IAM Process	Normative level Wbp	Normative level ISO 27001-2	Normative level GBA	Normative level PET	Minimum level without PET	Minimum normative level with PET
Authentication Management	Defined	Defined	Defined	Managed	Defined	Managed
User Lifecycle Management	Defined	Defined	Defined	Managed	Defined	Managed
Authorization Management	Managed	Defined	Defined	Managed	Managed	Managed
Access Management	Managed	Managed	Defined	Managed	Managed	Managed
Provisioning	Defined	Defined	Defined	Managed	Defined	Managed
Monitoring & Audit	Managed	Managed	Defined	Managed	Managed	Managed

Figure 11. Minimum normative maturity level requirements

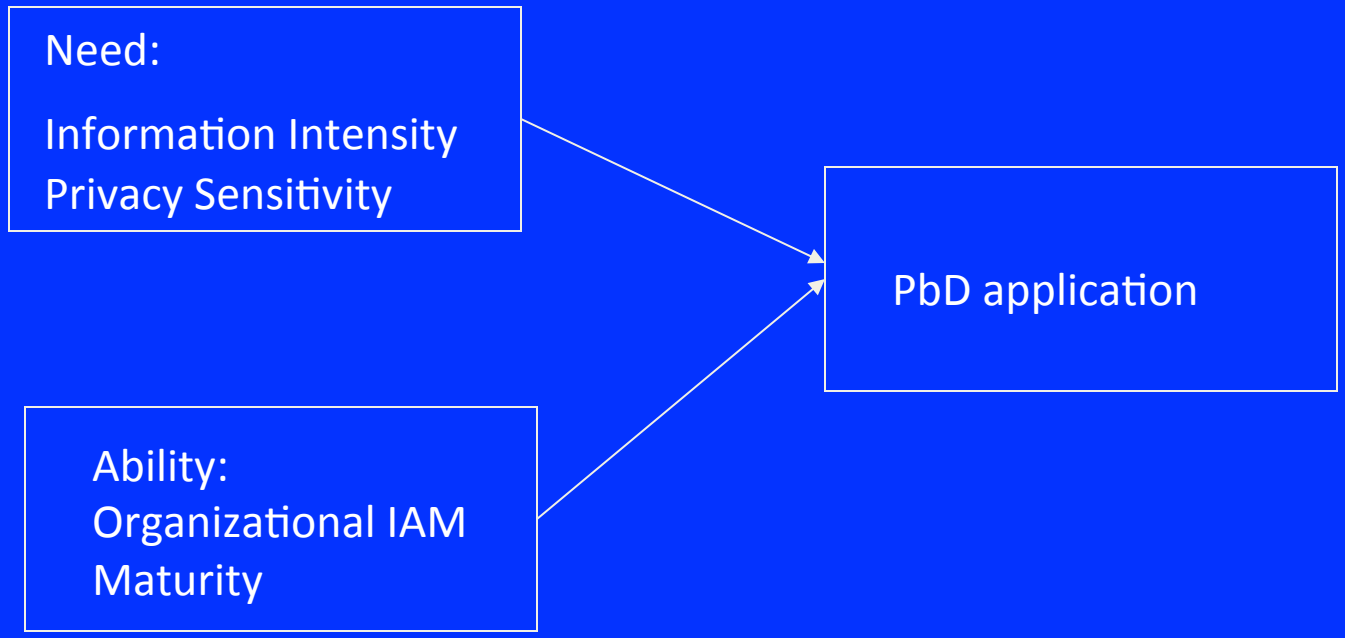
GAUGING EINDHOVEN



Actual Maturity levels at the Municipality vs. the normative maturity levels; **Green** represents GBA; **Purple** represents the Municipality of Eindhoven (2009) (De Kruijff, J.C, Identity & Access Management, A study to measures for successful implementation, Master Thesis University of Tilburg 2010)

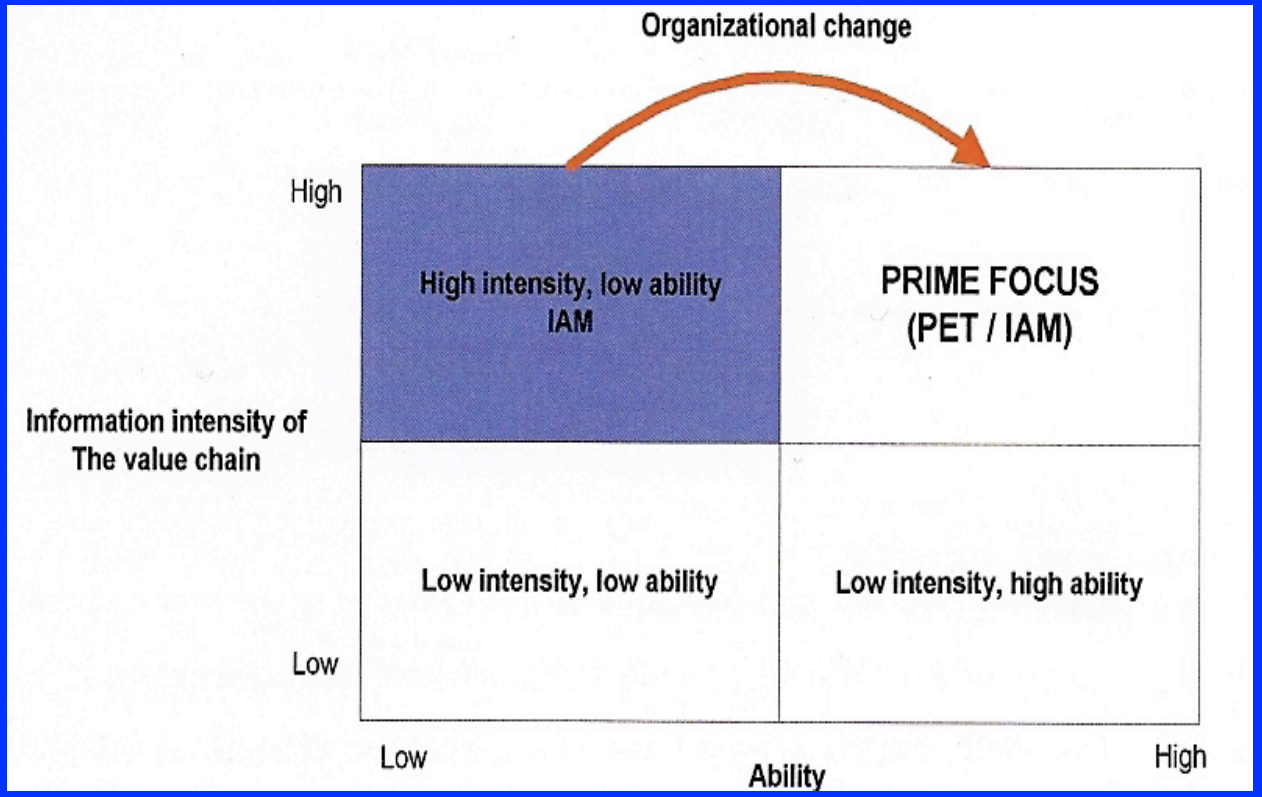
TOWARDS A TYPOLOGY

Typology determined by an Organization's need to apply a specific level of Privacy protection and its ability to do it



Ribbers P.M.A., Privacy Process Requirements & Privacy Implementation, Deliverables PRIME F 1 & PRIME F2, Brussels, 2007

POTENTIAL ORGANIZATIONAL CHANGE (Binary Combination Table)



CONCLUSIONS

- PbD: No one-size-fits-all solution
  - We need a toolbox with PIA, Privacy Design Patterns, PETs, PMS and design processes (Waterfall etc.) (More PKE research please)
  - Validate (use of) PbD-toolbox via design processes
  - We do need the collection of and publication of concrete examples to learn from and collect and create metrics for the consequences of PbD
  - PbD: Should facilitate certification of [product, production process, design], like certificates from EuroPrise & Certification should proof the presence of PbD (a sine qua non) (www. european-privacy seal.eu/ about europrise)
  - Use Adoption factors (promotion by EU & DPA) and maturity gauging; Four tracks policy should be leading in PbD policy making

References

- Borking J.J.F.M., Privacy Law is Code; About the deployment of privacy enhancing technologies, Leiden 2010 (Privacyrecht is Code; Over het gebruik van PET)
- Borking J.J., Why Adopting Privacy Enhancing Technologies (PETs) Takes So Much Time, , Dordrecht/Heidelberg 2011
- Camenish J., R.Leenes & D.Sommer (eds.) Privacy and Identity Management for Europe, Brussels, 2008
- Casassa Mont M., Privacy Models and Languages: Obligation Policies in J.Camenish, R.Leenes & D.Sommer, Privacy and Identity Management for Europe, Brussels 2008
- COM (2010) 245, A Digital Agenda for Europe, Brussels 2010
- Fritsch L., State of the art of Privacy Enhancing Technology (PET), Deliverable 2.1, PETWeb Research project, Oslo 2007
- IPC Ontario Toronto 2009, www.ipc.on.ca /images/Resoures/7 foundational principles
- De Kruijff, J.C, Identity & Access Management, A study to measures for successful implementation, Master Thesis, University of Tilburg 2010
- Rogers E.M., Diffusion of Innovations, 5th edition New York 2003
- Van Rest J. et all, Designing privacy-by-design, 1st Annual Privacy Forum, Limasol, 2012
- Ribbers P.M.A., Privacy Process Requirements, Deliverable PRIME F 1 & F 2, Brussels 2007
- Hes R. & J.Borking, Privacy-Enhancing Technologies,The Hague 2000
- WP 168 The Future of Privacy , Brussels 2009
- Van Lieshout M., Stimulerende en remmende factoren van Privacy -by -Design in Nederland, The Hague 2012

THANK YOU