Privacy management practices in the proposed EU Regulation

Prof. Dr. Rolf H. Weber

Chair for International Business Law, University of Zurich and Hong Kong

Bratschi Wiederkehr & Buob AG, Zurich, Attorney at law

Brussels (VUB), October 28, 2014

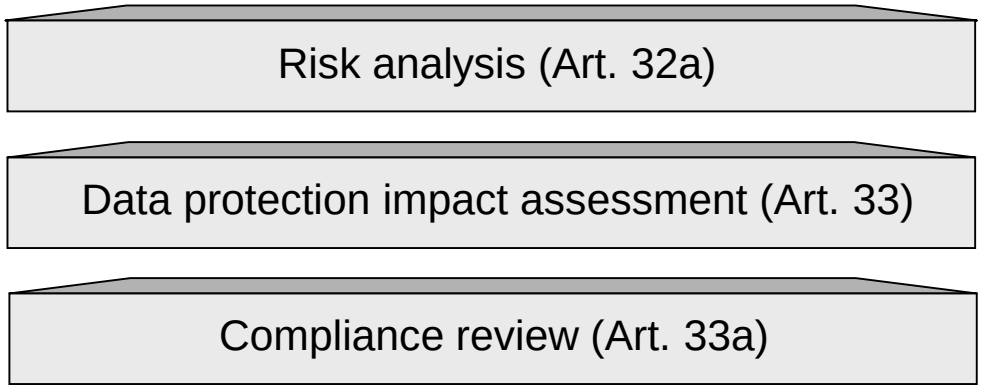
Notions

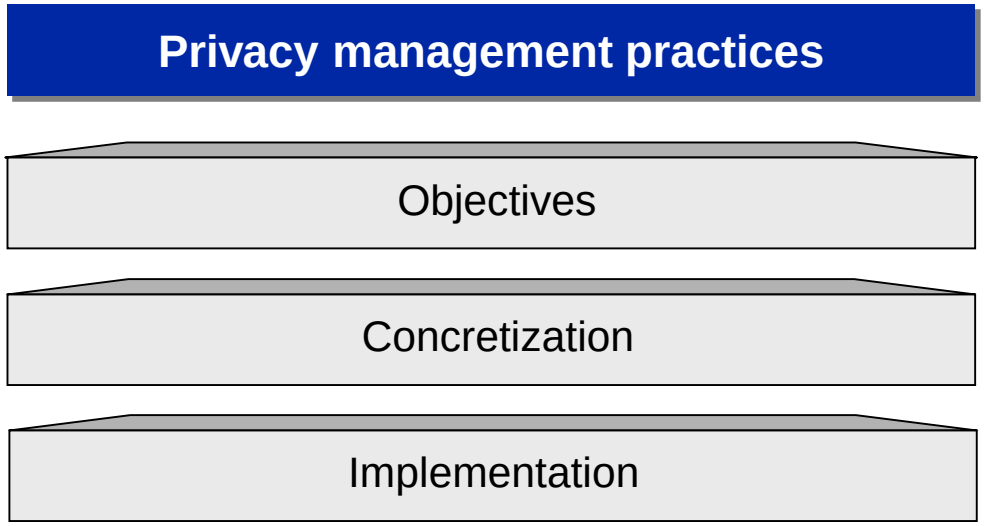
Development of privacy regulations

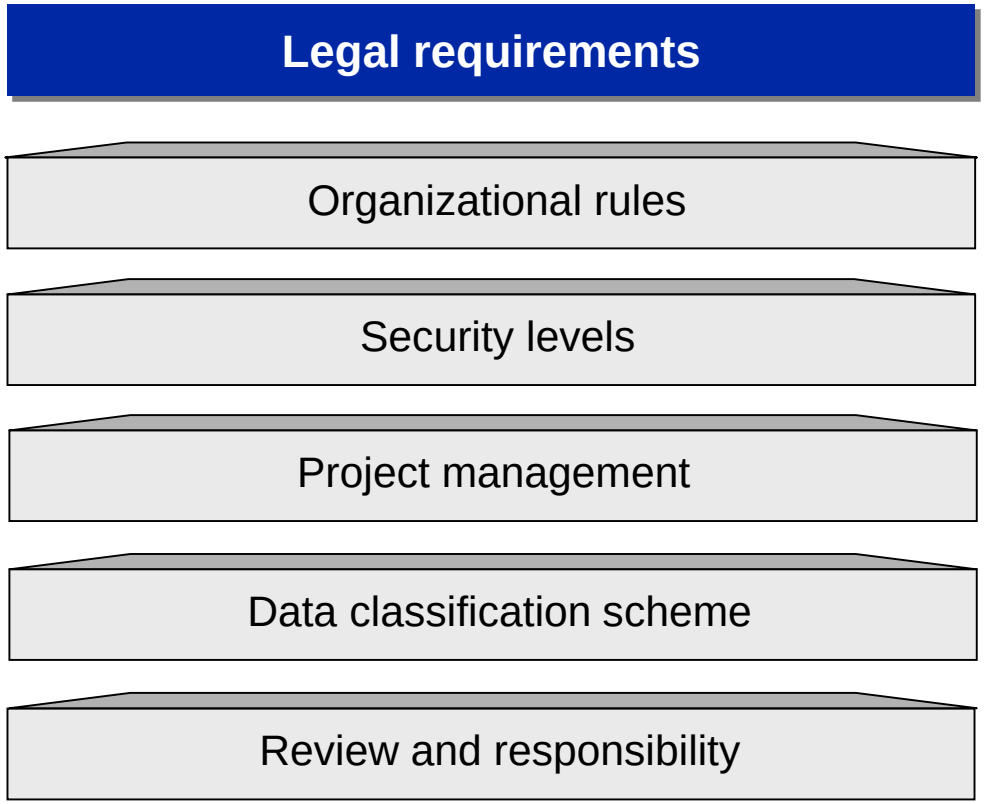
From program to framework

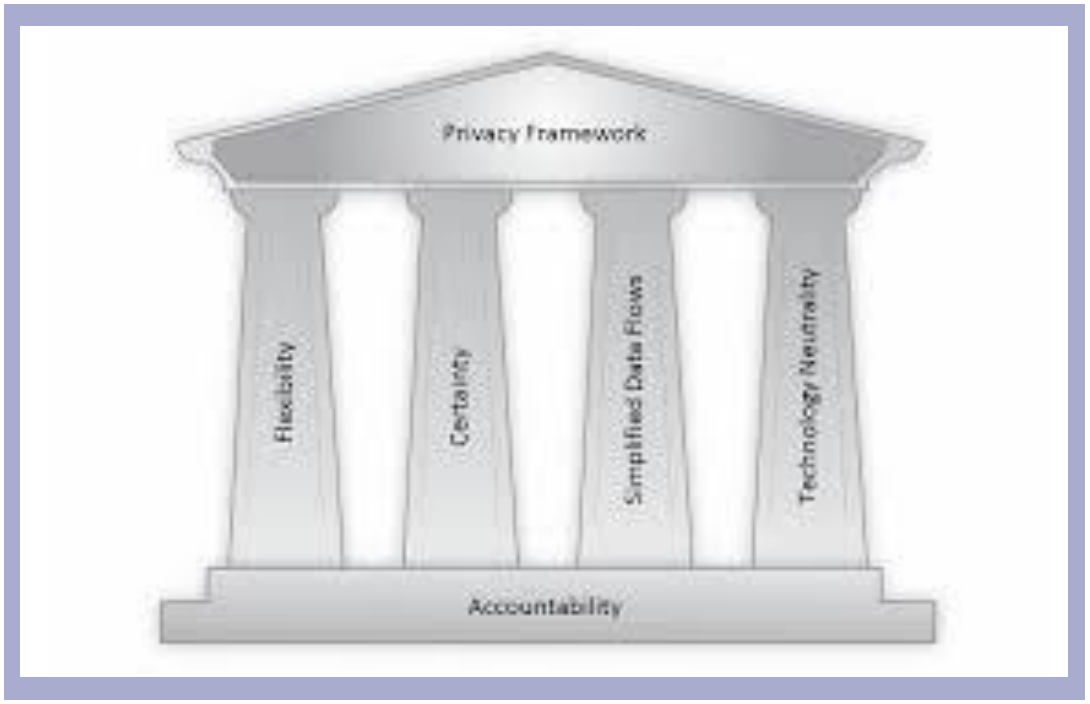
Legal embedment

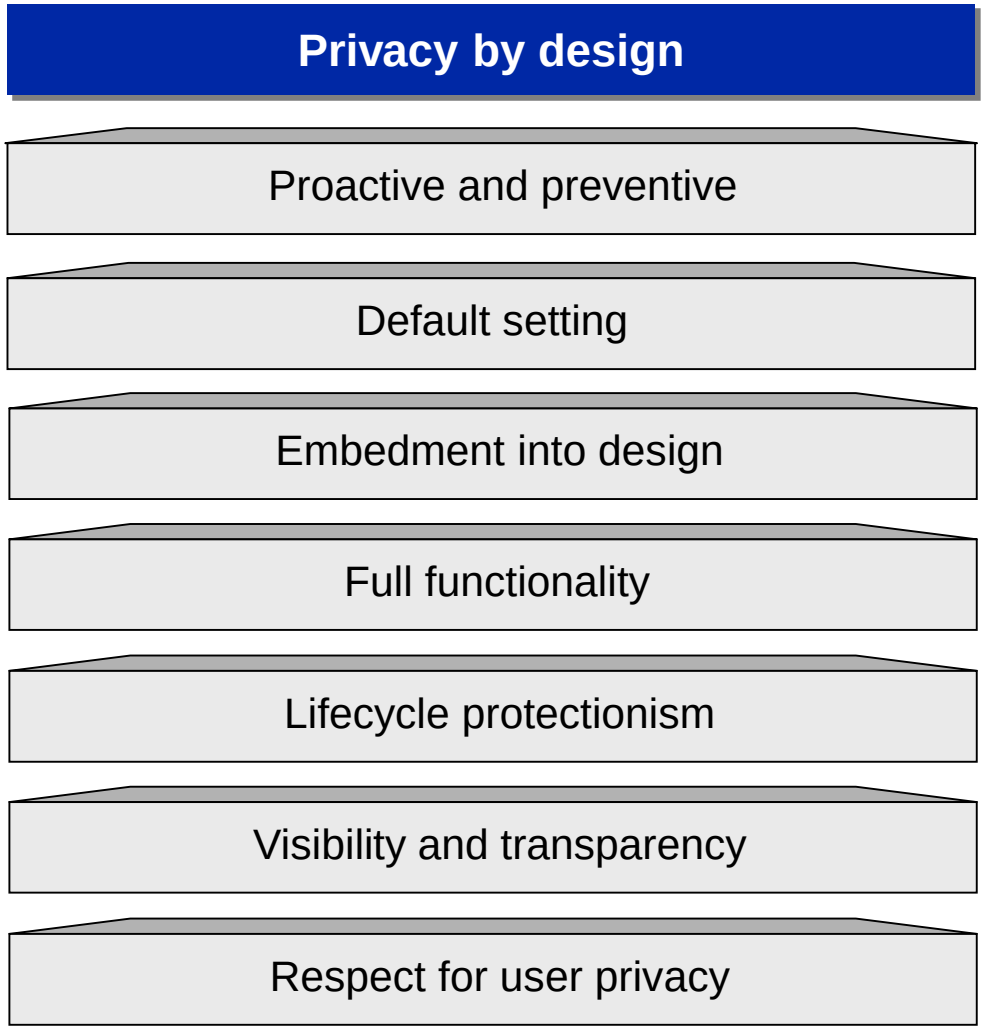
New Provisions in the EU-DPR




Privacy management practices
Objectives
Concretization
Implementation

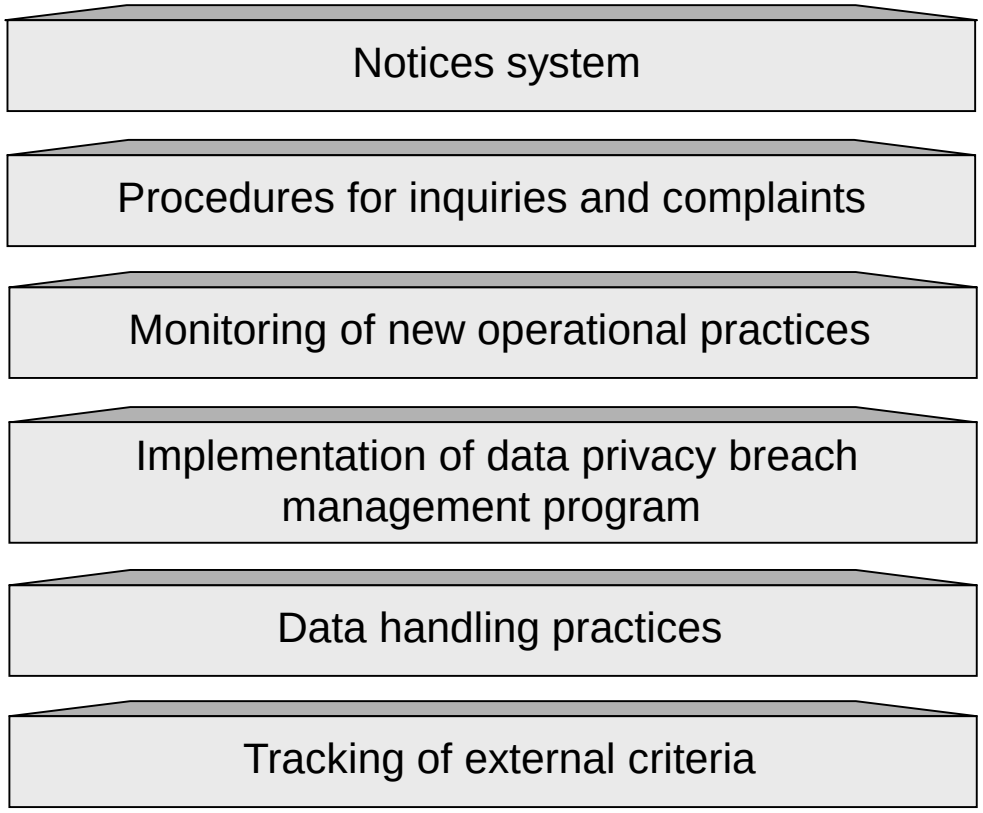

Legal requirements
Organizational rules
Security levels
Project management
Data classification scheme
Review and responsibility


Privacy Framework
Flexibility
Certainty
Simplified Data Flows
Technology Neutrality
Accountability


Privacy by design
Proactive and preventive
Default setting
Embedment into design
Full functionality
Lifecycle protectionism
Visibility and transparency
Respect for user privacy

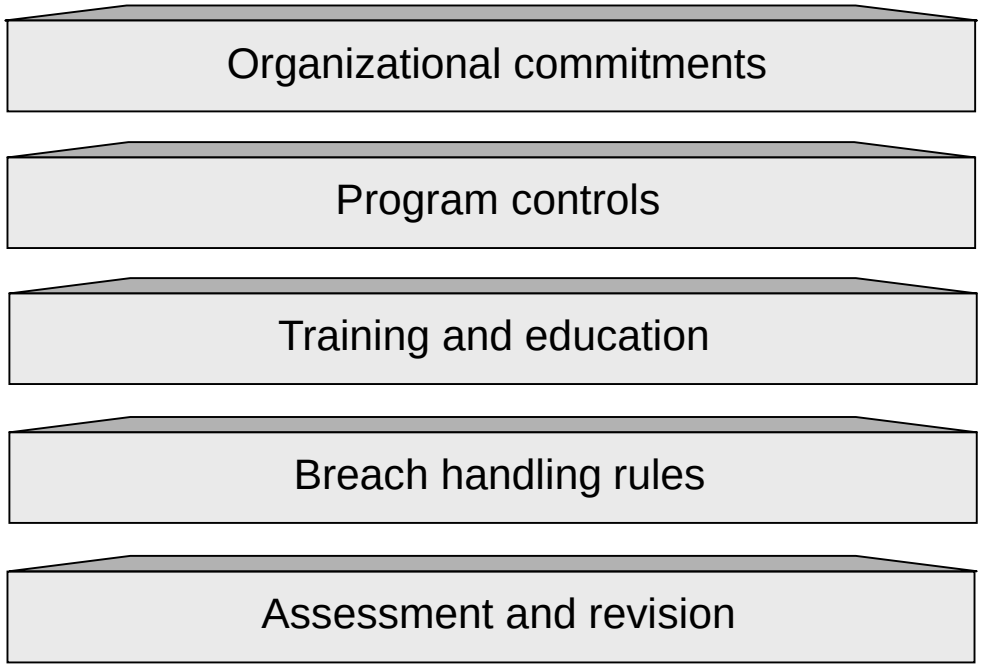
Privacy accountability framework I

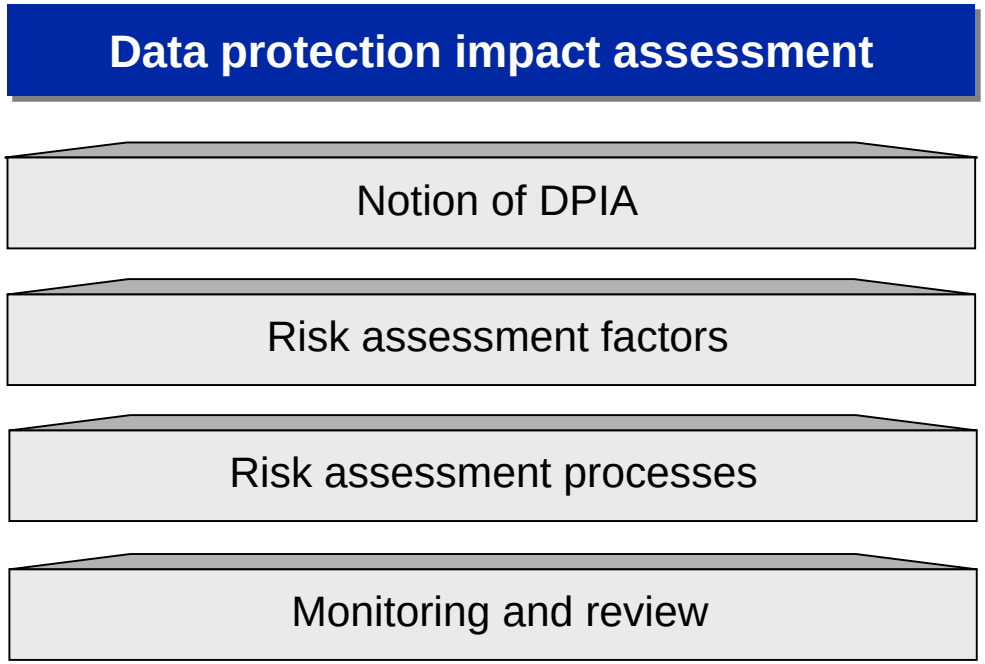
Privacy accountability framework II




ASSESS
CONTROL
CERTIFY
MONITOR

Example Hong Kong




Data protection impact assessment
Notion of DPIA
Risk assessment factors
Risk assessment processes
Monitoring and review

Assessment of DPR provisions

- Enlarging the scope of processing operations?
- Improving transparency and accountability?
- Requiring budgets and specific safeguards?
- Including external experts?
- Extending regulatory flexibility?


ASSESS
TRUSTe
MONITOR
CONTROL
Enterprise Dashboard
Data Privacy Management Platform

Further recommendations

- Harmonization of terminology / methodology and list of minimum applicable variables
- Definition of scope of relevant data
- Application of SWOT-analysis
- Limitation of exception rule
- Transparency and “public notice”
- Development of self-assessing tools