



**University of
Zurich^{UZH}**

Law Institute

**bratschi
wiederkehr
& buob**

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 embedding



New Provisions in the EU-DPR

Risk analysis (Art. 32a)

Data protection impact assessment (Art. 33)

Compliance review (Art. 33a)



Privacy management practices

Objectives

Concretization

Implementation



Legal requirements

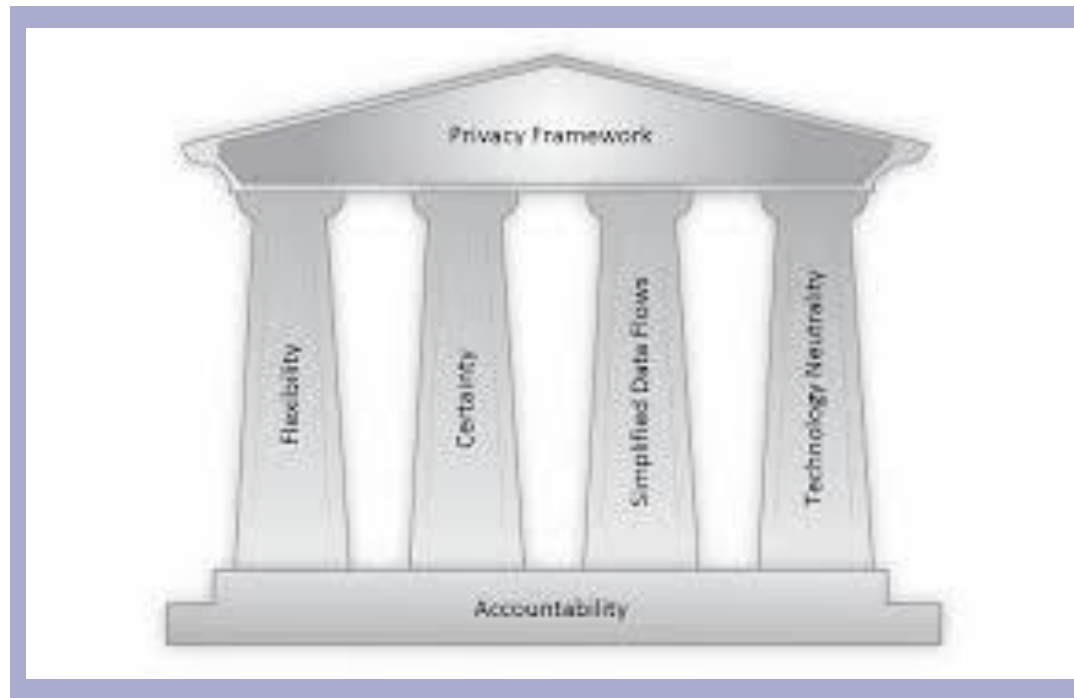
Organizational rules

Security levels

Project management

Data classification scheme

Review and responsibility





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

Governance structure

Personal data inventory

Data privacy policy

Operalization of data policy

Training and education program

Management of information security risks

Management of third-party risks



Privacy accountability framework II

Notices system

Procedures for inquiries and complaints

Monitoring of new operational practices

Implementation of data privacy breach
management program

Data handling practices

Tracking of external criteria





Example Hong Kong

Organizational commitments

Program controls

Training and education

Breach handling rules

Assessment and revision



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?





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