Swiss Re

General Public Release

Privacy by design - Challenges in global information communication systems

Goethe University, 21 January 2015

Agenda

- Speaker Introduction
- Privacy by Design
- Challenges
- Use Case – Cloud Computing
- Q&A

Speaker Introduction

Dr. Stefan Weiss
Professional Background

since November 2011
- Global Data Protection Officer, Swiss Re, based in Zurich/Switzerland

Previously (for 10 years):
- Director, Risk Consulting, KPMG, Frankfurt/Germany
- Senior Manager, Security & Privacy Services, Deloitte, Frankfurt/Germany
- and with security consulting firms @stake and Defcom Security

Education:
- PhD, Goethe University, Frankfurt/Germany (2004-2009)
- BBA & MBA from The George Washington University, Washington D.C./USA

Professional and Academic Activities:
- Certified Information Privacy Professional and IAPP Member (since 2007)
- Project Editor of Privacy Standards with ISO JTC1, SC 27, WG5 (since 2006)
- Research Fellow, Data Protection, Goethe University, Frankfurt/Germany
- Speaker for the Working Group on Privacy-Enhancing-Technologies in the ‘Gesellschaft für Informatik‘ (GI e.V.)

Dr. Stefan Weiss
Academics

Doctorial thesis at Goethe University (m-chair) in 2009

- An Information Architecture Framework for Enhancing Privacy in Social Network Applications

Research Interests:

- Data protection and privacy
- Privacy-enhancing technologies
- Social network applications
- Big data

Topics for speaking engagements:

- Privacy compliance and business strategy
- Corporate data protection management
- Trust and security of social networks - on data portability and privacy
- International data protection standardization

Privacy by Design

Privacy – Myth or fact?

Myth:

"I have nothing to hide"

"Privacy is dead"

"Silly old farts"

Fact:

ECHR, Article 8

EU Court of Justice, C-131/12

"Users care more about privacy then they would expect"

Privacy defined (1)

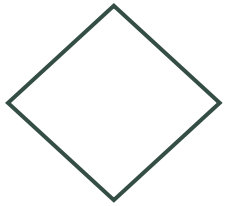
Westin (1970) defined privacy as

"being the claim of individuals, groups, or institutions to **determine for themselves** when, how, and to what extent information about them is communicated to others."

Privacy in the context of information systems:

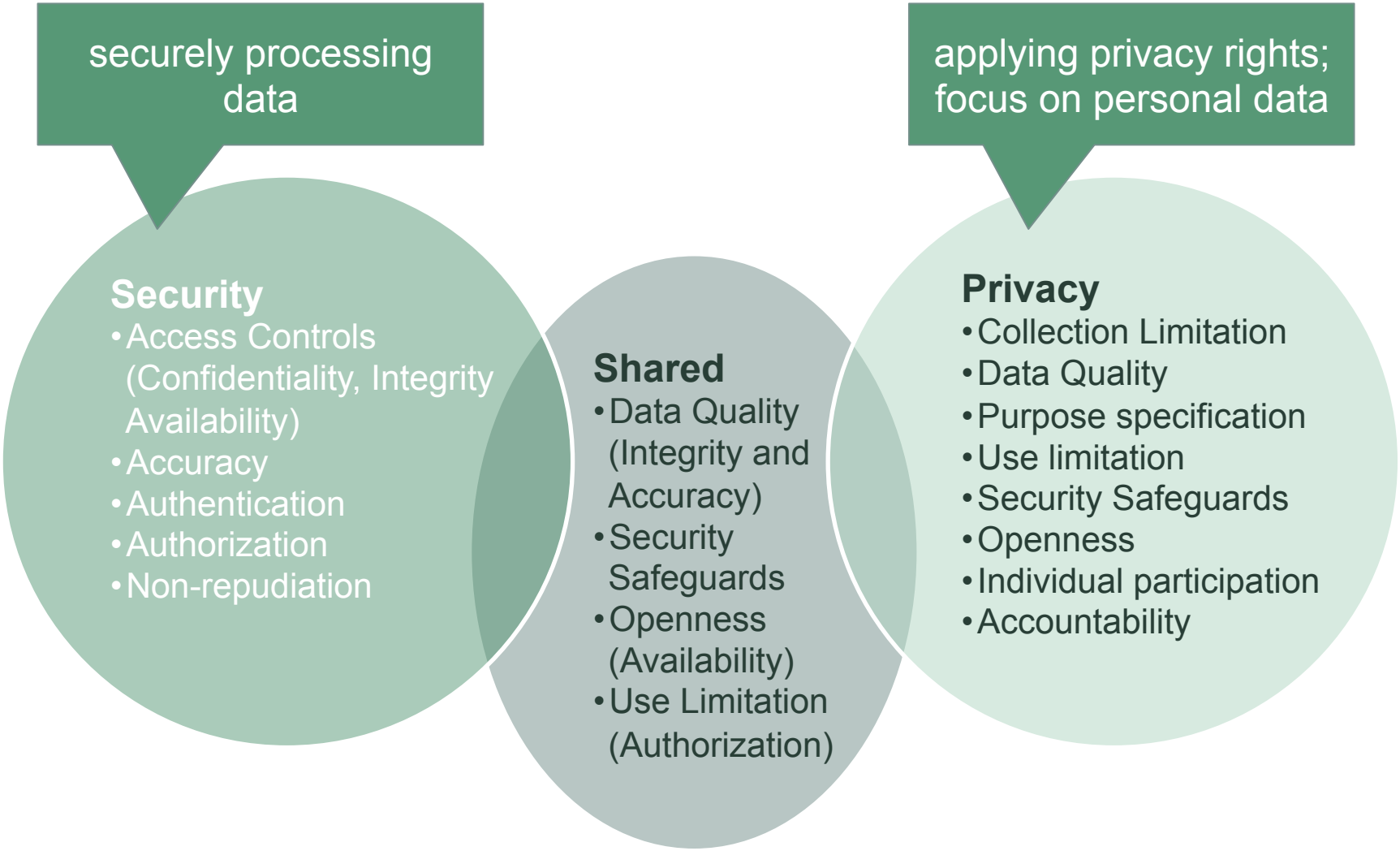
Personal data

Control



Data processes

The Security-Privacy Paradox (2)



What is 'Privacy by Design' (PbD)?

The objectives of *Privacy by Design* are twofold:

1. **for the data subject (user):** ensuring privacy and gaining personal control over one's information and
2. **for organizations:** implementing controls that can mitigate against data protection and privacy compliance risks

Privacy by Design is

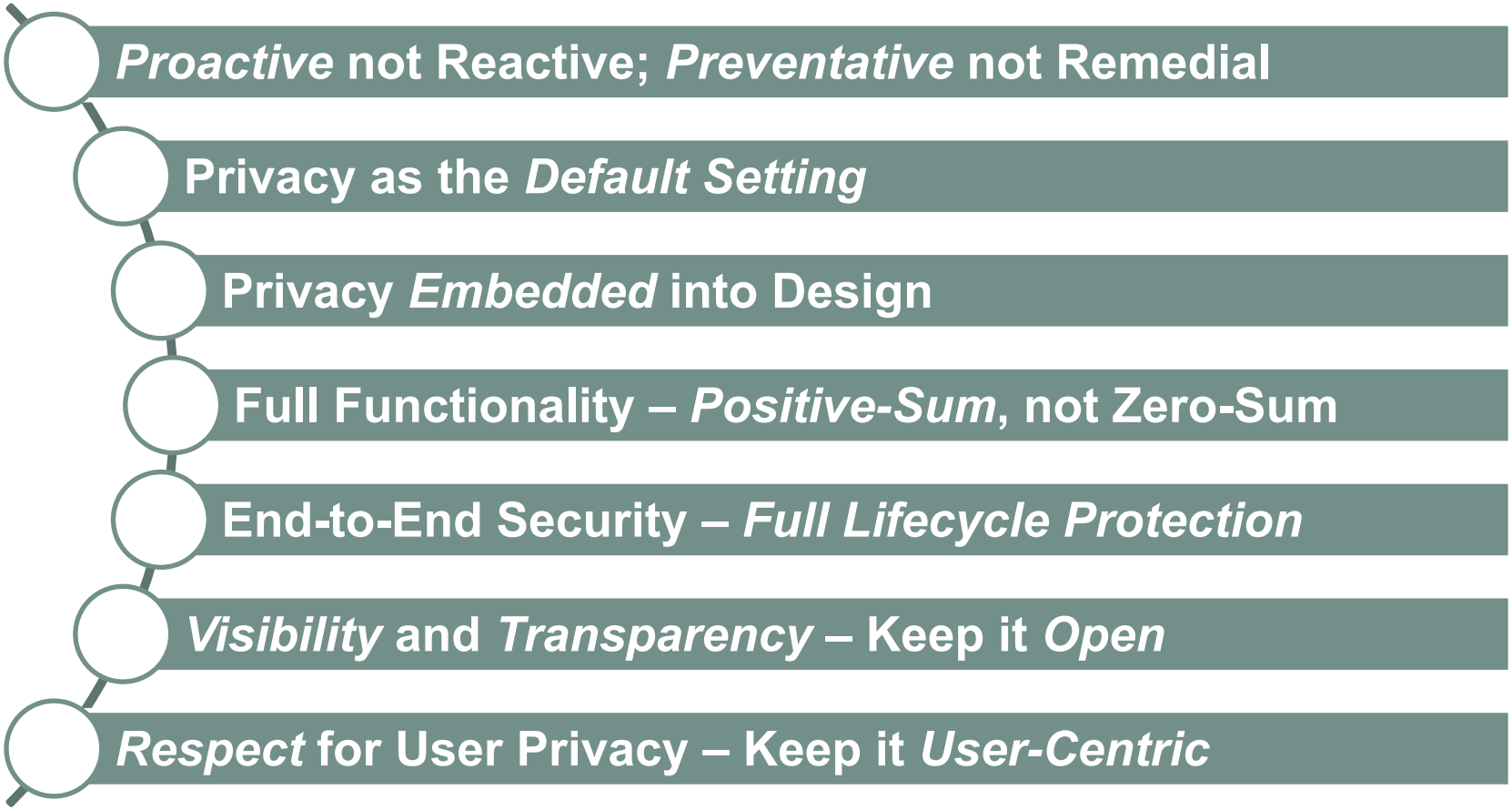
- a holistic concept that may be applied to operations throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure *(as defined in 2010 by the 32nd International Conference of Data Protection and Privacy Commissioners)*

"Trust, or rather its absence, has been identified as a core issue in the emergence and successful deployment of information and communications technologies.

If people do not trust ICT, these technologies are likely to fail. … Such trust will only be secured if ICTs are reliable, secure, under individuals' control and if the protection of their personal data and privacy is guaranteed.
To significantly minimize the risks and to secure users' willingness to rely on ICTs, it is crucial to integrate, at practical level, data protection and privacy from the very inception of new ICTs."

Peter Hustinx, European Data Protection Supervisor, 2010

Privacy by Design Principles (3)



Challenges

How is PbD perceived in the corporate world?

Forbes | New Posts +16 | Most Popular | Lists | Video | 2 Free Issues of Forbes

Log in | Sign up | Privacy | Terms | AdChoices | Help

Kashmir Hill
Forbes Staff

FOLLOW

Welcome to The Not -So Private Parts where technology & privacy collide
full bio →

TECH 7/28/2011 @ 1:23PM | 6,862 views

Why 'Privacy By Design' Is The New Corporate Hotness

+ Comment Now + Follow Comments

How can companies with lots of sensitive data about us strive for "privacy by design" instead of "embarrassment by design"? After Fitbit.com fell into the latter camp by failing to foresee the downside of making its users' activity-tracking-journals public by default (when one of the 800 activities users tracked was S-E-X), I reached out to Ontario Information and Privacy Commissioner Ann Cavoukian, who has been pushing companies since the 1990s to embrace the concept of "privacy by design."

"Stories like that one are why one of the core principles of 'privacy by design' is for companies to make users' data private by default," says Cavoukian.

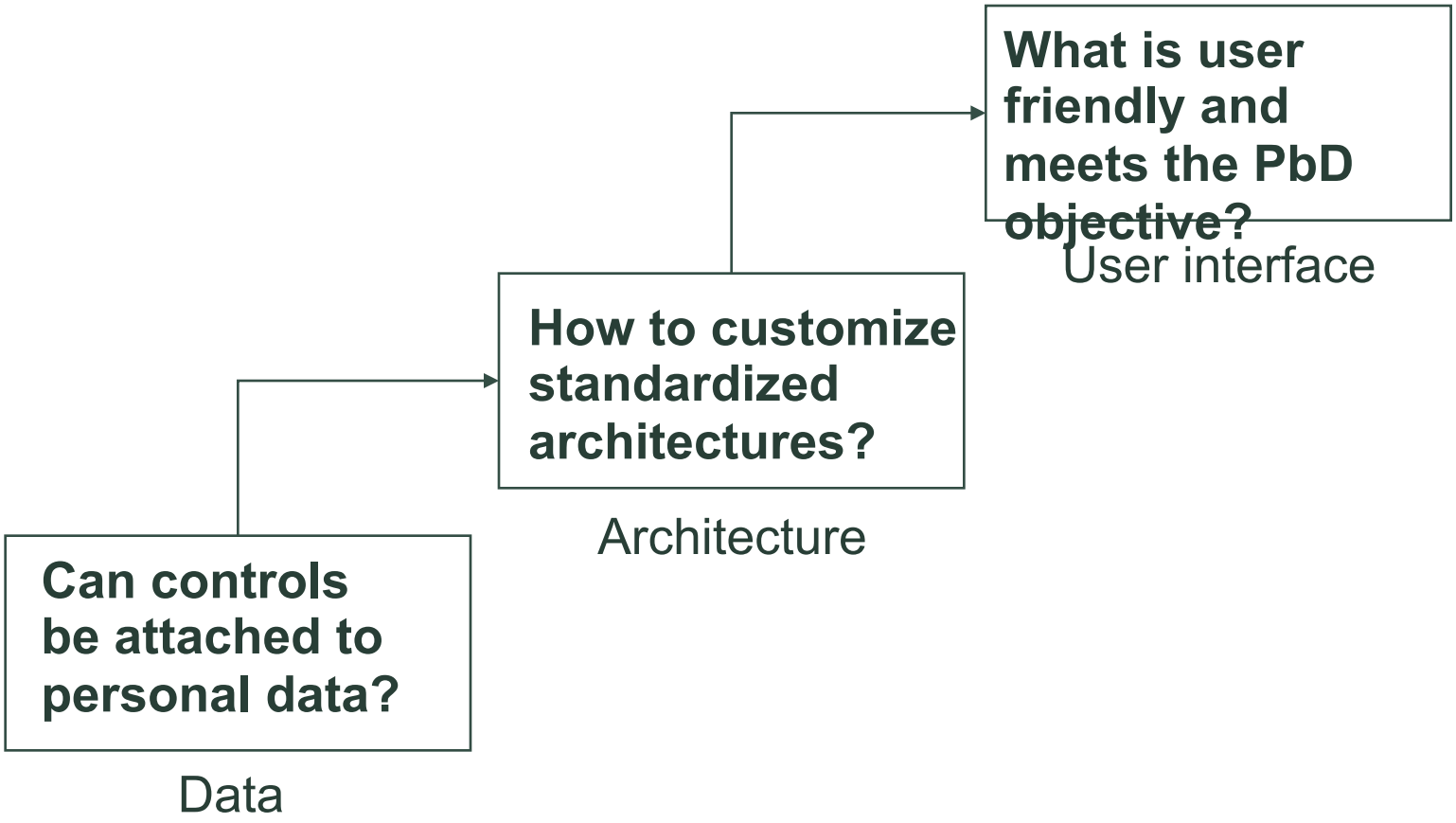
Ann Cavoukian, 'Privacy by

- Source: Kashmir Hill, Forbes Magazine, 28 Jul 2011, at http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/

Challenges for implementing PbD

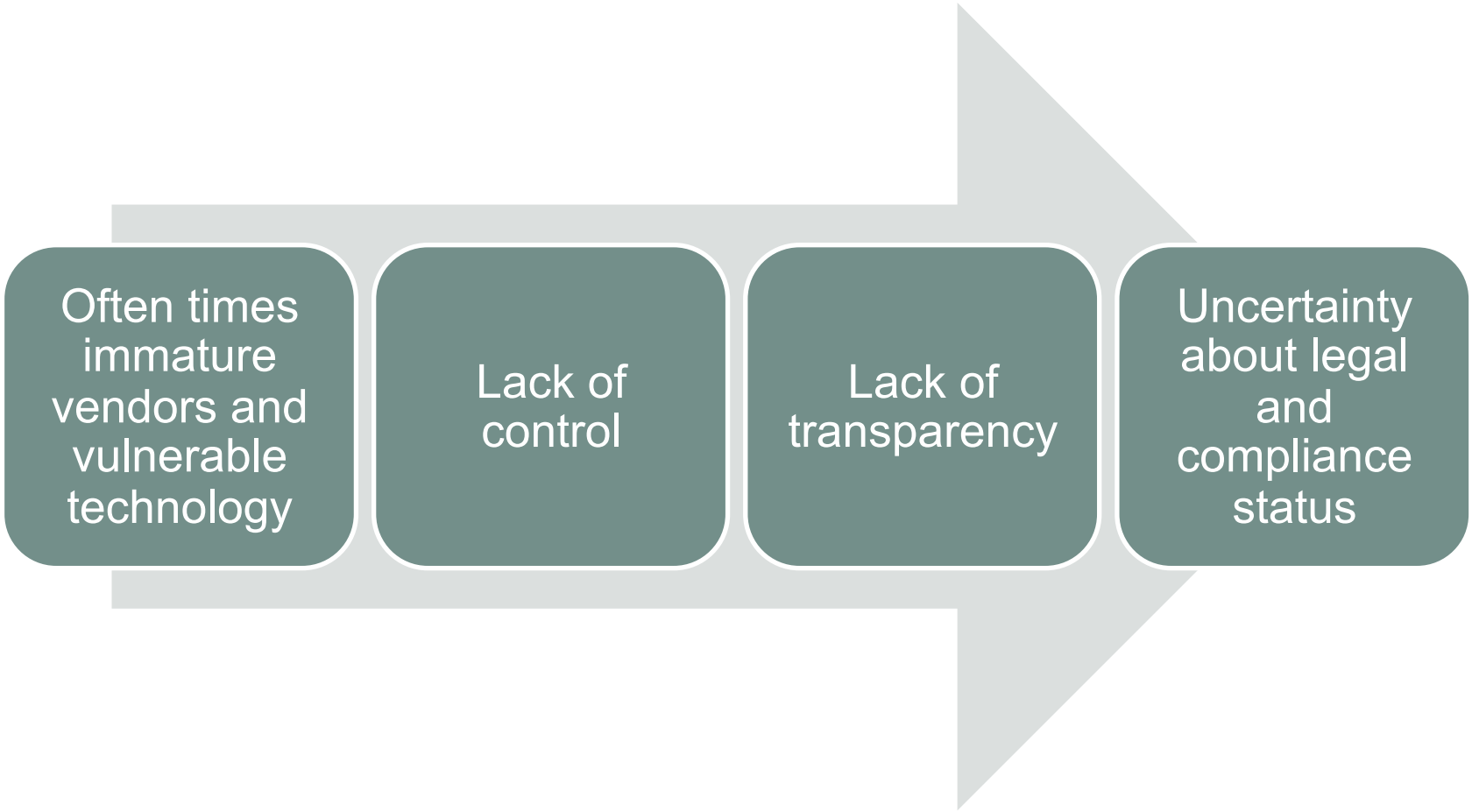
- Unawareness and perception (architects, developers)
- Security-Privacy-Paradox (security vs. privacy)
- Lack of technical solutions (PETs)
- Complexity of data processing (sources, purposes)
- Multilateral interactions (stakeholders)
- Interdependencies (infrastructure, application)

Challenges on different levels

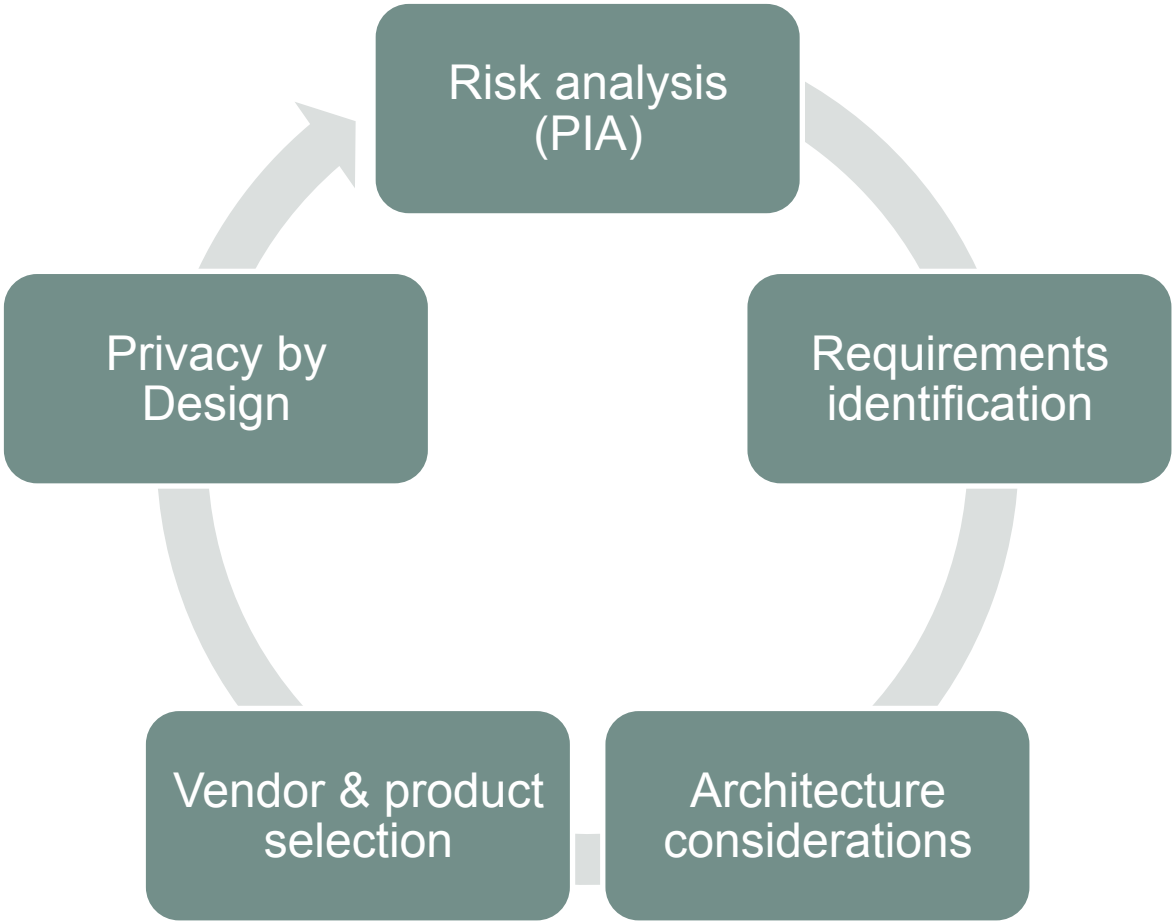


Use Case – Cloud Computing

Risks with cloud computing



Simplified design process for cloud implementation



Examples for factors that need to be considered

- Risk analysis
  - PIA determines sensitivity of data and any potential impact on an individual
- Requirements identification
  - Legal, regulatory, internal and business-related requirements
- Architecture considerations
  - Integration into existing environment, stand-alone/external, private vs. public
- Vendor & product selection
  - Contractual arrangements, jurisdictional scope, solution flexibility
- Privacy by Design
  - Notifications to users, consent mechanisms, data minimization, self-servicing (user control), security features, pseudonyms etc.

Contact and Resources

Contact information

Dr. Stefan Weiss
Global Data Protection Officer
Director, Legal & Compliance
Swiss Reinsurance Company Ltd
Mythenquai 50/60
8022 Zurich, Switzerland
Direct: +41 43 285 4448
Mobile: +41 79 207 3142
E-mail: Stefan_Weiss@swissre.com

http://www.swissre.com

Resources and Bibliography

- Academic information / Speaker engagements:

  http://www.stefanweiss.net/_/Profession.html

Bibliography:

(1) *Westin, Alan F.* (1970): Privacy and Freedom, The Bodley Head Ltd., London, UK

(2) *Deloitte & Touche LLP* (2003): The Security-Privacy Paradox – Issues, Misconceptions and Strategies

(3) *Information Privacy Commissioner Ontario*, Canada, 7 Foundational Principles of Privacy by Design
http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

Q&A

Questions and Answers / Discussion Session

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.