Transparency and accountability
... and more ... in the Cloud

- Input Statement -

Marit Hansen
Data Protection Commissioner Schleswig-Holstein,
Kiel, Germany

Limassol, 27 April 2017

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Source: en.wikipedia.org/wiki/Schleswig-Holstein
Source: www.maps-for-free.com
**ULD focus: data protection by design**

- Motivation for joining R&D projects or discussing with researchers
- Objective:
  - Exploring and broadening the solution space
  - Bridging the gap between research and practice, as well as the expertise of DPAs
  - Involving multiple disciplines
- Working with the Standard Data Protection Model*)

*) [https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methodology_V1_EN1.pdf](https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methodology_V1_EN1.pdf)

**Protection goals: more than IT security**

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

classical IT security protection goals*)

*) From the data subject's perspective

- Compliance
- Contractual safeguards
- Technical and organisational measures of data protection and data security

- Availability
- Integrity
- Confidentiality
- Transparency
- Isolation (purpose limitation; unlinkability)
- Intervenability (data subject rights)
- Portability
- Accountability

Not only adding measures on top, but building in data protection (Art. 25 GDPR)

A4Cloud: Accountability for controllers

Chain of Accountability

Cloud service supply chain/network

Preventive: e.g. DPIA tool
Detective: e.g. Data transfer monitoring tool
Corrective: e.g. Incident management tool

Jurisdiction? Gov. access?

Reference: A4Cloud project, based on slides from Simone Fischer-Hübner
A4Cloud: Transparency for users

Complex system of data flows – hard to check for users
⇒ Data Track for transparency & intervenability

http://dx.doi.org/10.1145/2702613.2732701

Multi-Cloud Approach (1/3)

Redundancy ⇒ higher availability

References:
TClouds (2012): Cloud Computing – Solutions and Enablers, Deliverable D1.2.3 (see http://tclouds-project.eu/);
Multi-Cloud Approach (2/3)

Separation of (personal) data ⇒ data minimisation

References:
TClouds (2012): Cloud Computing – Solutions and Enablers, Deliverable D1.2.3 (see http://tclouds-project.eu/);

Multi-Cloud Approach (3/3):

Separation of processes ⇒ data minimisation

References:
TClouds (2012): Cloud Computing – Solutions and Enablers, Deliverable D1.2.3 (see http://tclouds-project.eu/);
Trustworthy Cloud: Secure Partitioning (1/2)

Deficiencies:
- Too little isolation
- Too powerful admins
- Internal attacks not prevented

References:

Fig. 1: SaaS Cloud Infrastructure architecture today: no isolation of users, user data and administrators

Trustworthy Cloud: Secure Partitioning (2/2)

Possible:
- Strict isolation
- Service maintenance without access to user data
- Solution uses encrypted security kernels

References:

Fig. 2: SPLITCloud architecture – strict isolation and Service Maintenance without access to user data
Combination with “Sealed Cloud”

Protection in the data centre:

- For controlled administration: sealed racks, reports on status information
- For confidentiality: erasure of unencrypted data as “fail-safe” mode

Result:
1. Data transfer to Sealed Cloud is protected
2. Data memory within Sealed Cloud is protected
3. Data processing within Sealed Cloud is protected

Transparency and accountability in the Cloud

Reference: http://www.sealedcloud.de/

Conclusion

- More “data protection by design” possible, e.g. R&D project results:
  - Tools for accountability
  - ... supported by strict isolation
  - ... and extra data centre security
  - Design for data minimisation
  - Tools for transparency

- Combination of technological, organisational, and contractual solutions

- Necessary: bridging the gap between research and practice
Thank you for your attention!

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel, Germany

https://www.datenschutzzentrum.de/

References

• Standard Data Protection Model

• Art. 29 Working Party: Opinion 05/2012 on Cloud Computing

• Selection of Cloud projects
  • A4Cloud: www.a4cloud.eu/
  • TClouds: www.tclouds-project.eu/
  • SPLITCloud: www.splitcloud.de/
  • Sealed Cloud: www.sealedcloud.de/