Transparency and accountability … and more … in the Cloud

– Input Statement –

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

Limassol, 27 April 2017

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Setting of ULD

Schleswig-Holstein	
State of Germany	
Flag / Coat of arms	
Coordinates: 54°28'12"N 9°30'50"E	
Country	Germany
Capital	Kiel
Government	
• Minister-President	Torsten Albig (SPD)
• Governing parties	SPD / Greens / SSW
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km² (6,086.20 sq mi)
Population (2015-12-31)[1]	
• Total	2,858,714
• Density	180/km² (470/sq mi)

Source: en.wikipedia.org/wiki/Schleswig-Holstein

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

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*)

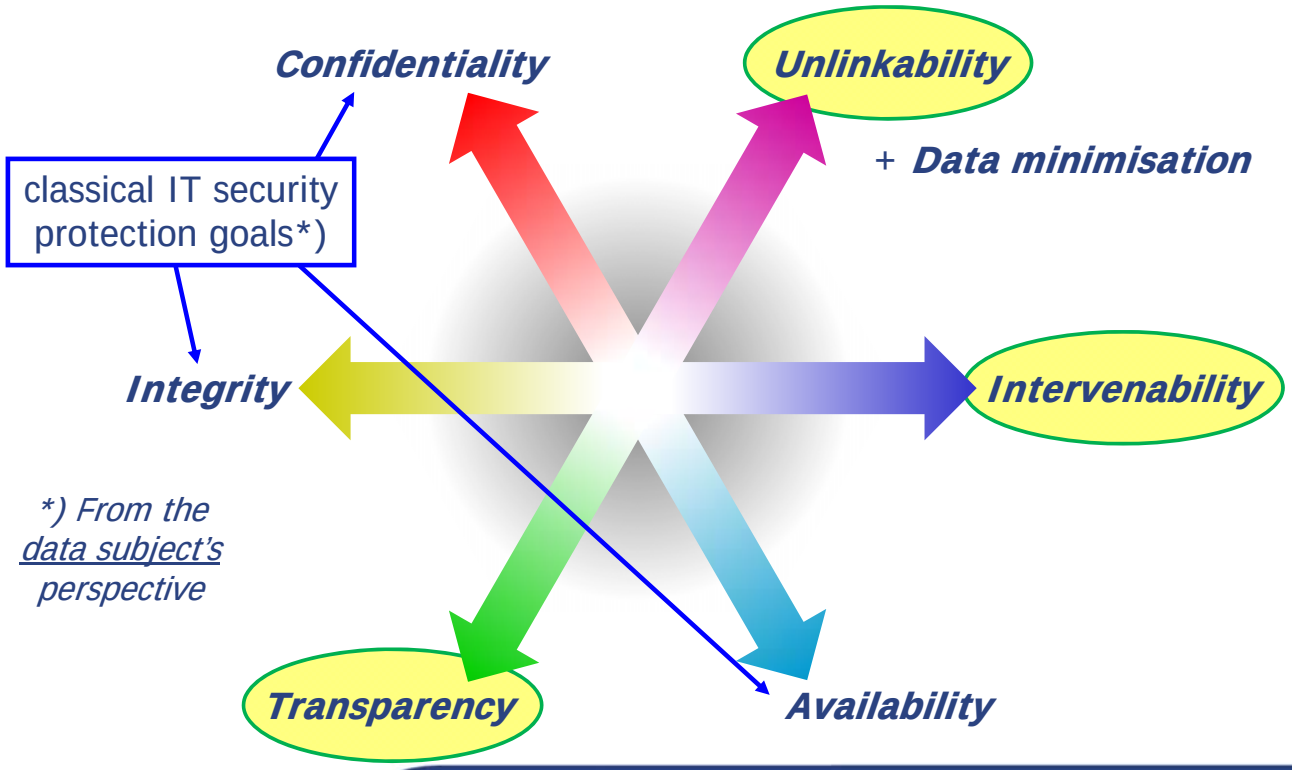
TClouds http://www.tclouds-project.eu/

CLOUD ACCOUNTABILITY PROJECT http://www.a4cloud.eu/

SPLIT Cloud http://www.splitcloud.de/

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

Protection goals: more than IT security



Art. 29 Working Party Opinion on Cloud Computing (2012)

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

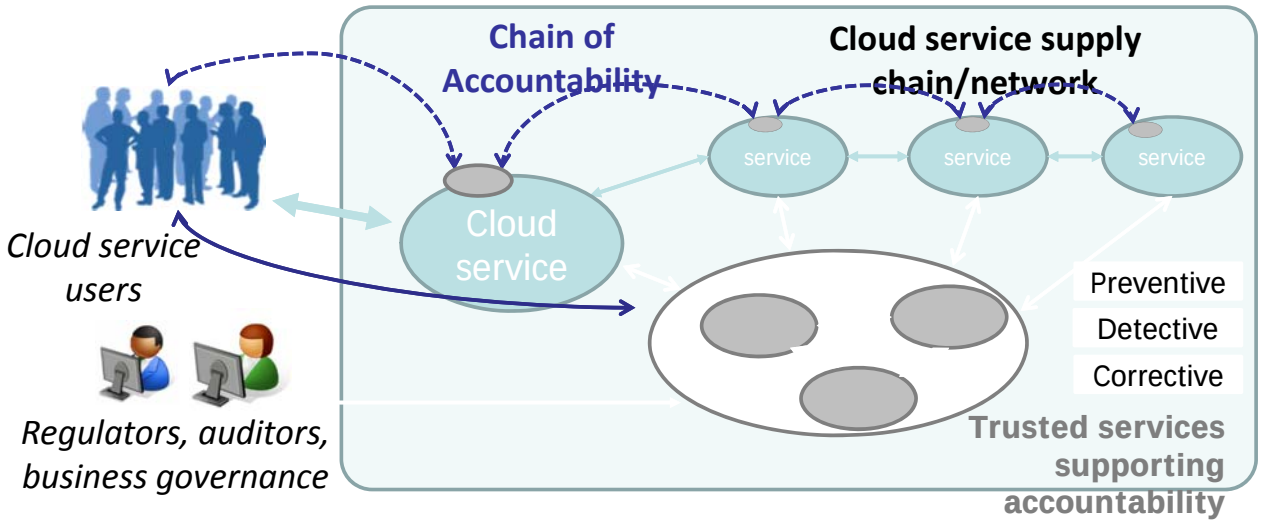
Cf. protection goals

- 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)

CLOUD ACCOUNTABILITY PROJECT
http://www.a4cloud.eu/

A4Cloud: Accountability for controllers



Jurisdiction?
Gov. access?

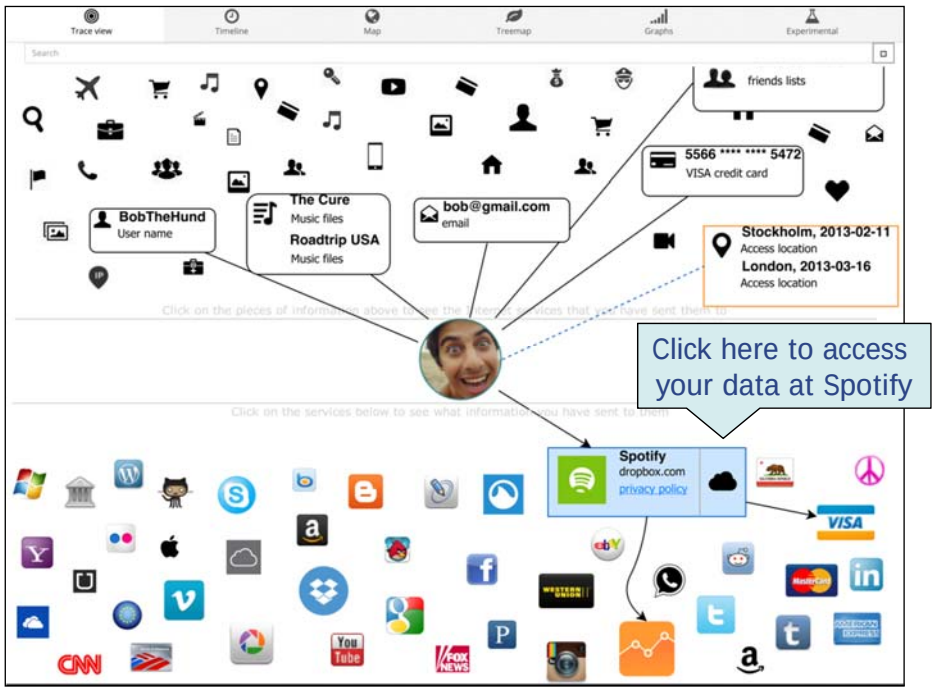
Preventive: e.g. DPIA tool
Detective: e.g. Data transfer monitoring tool
Corrective: e.g. Incident management tool

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

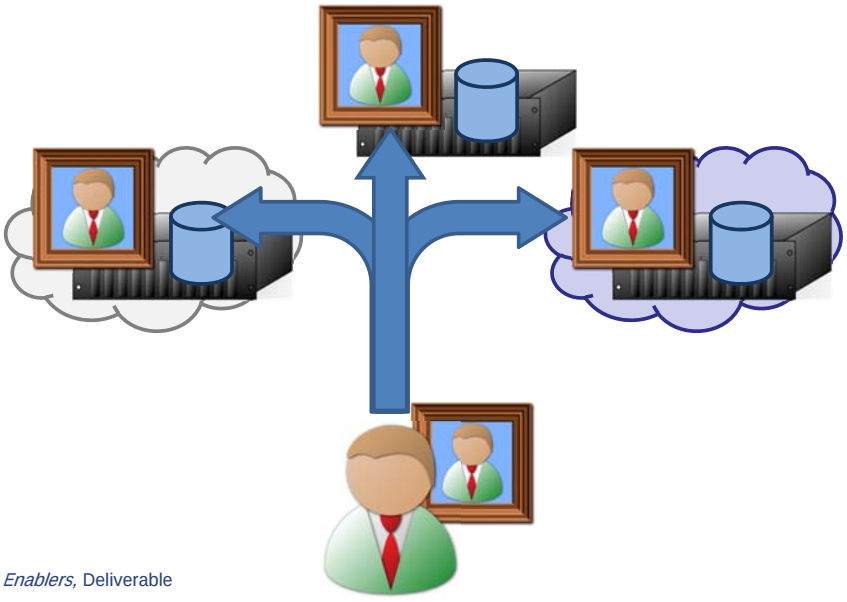


Reference: Angulo et al. (2015): Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures, CHI EA '15 http://dx.doi.org/10.1145/2702613.2732701

TClouds
http://www.tclouds-project.eu/

Multi-Cloud Approach (1/3)

Redundancy ⇒ higher availability

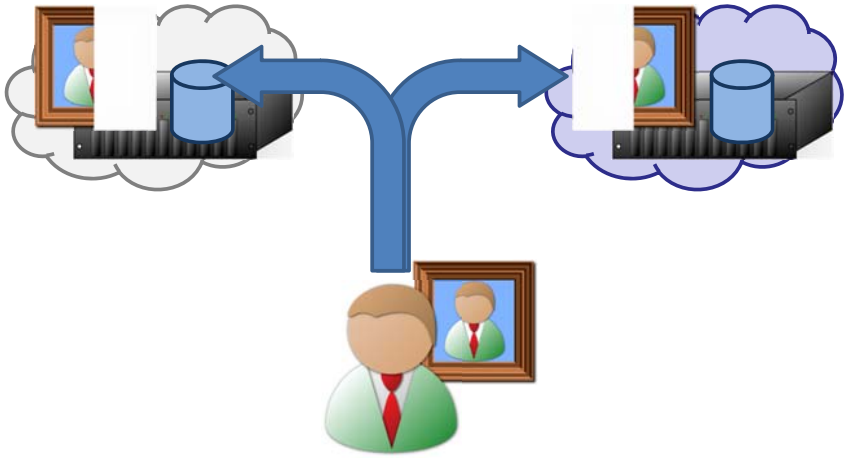


References:
TClouds (2012): *Cloud Computing – Solutions and Enablers,* Deliverable D1.2.3 (see http://tclouds-project.eu/);
M. Jensen, J. Schwenk, J.-M. Bohli, N. Gruschka, L. Lo Iacono (2011): *Security Prospects through Cloud Computing by Adopting Multiple Clouds*, Fourth IEEE International Conference on Cloud Computing, pp. 565-572.

TClouds
http://www.tclouds-project.eu/

Multi-Cloud Approach (2/3)

Separation of (personal) data ⇒ data minimisation

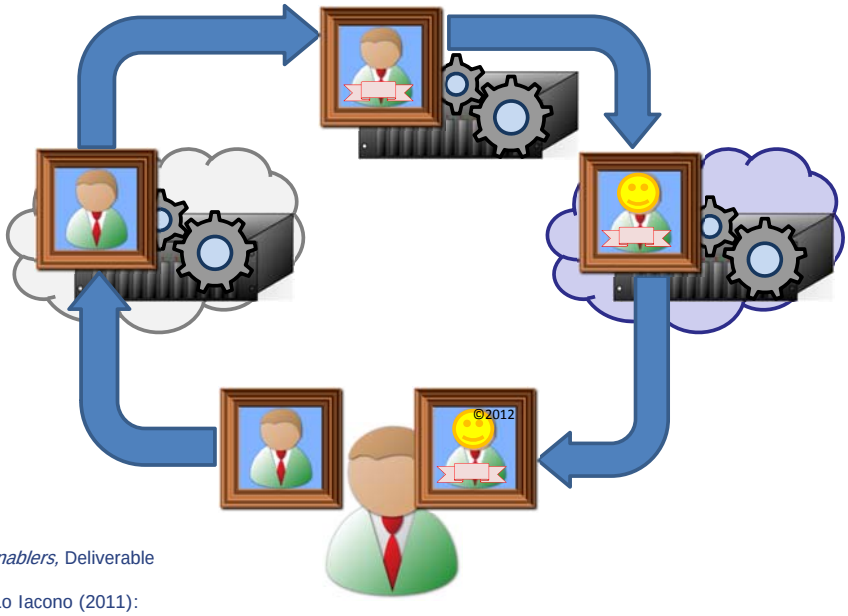


References:
TClouds (2012): *Cloud Computing – Solutions and Enablers,* Deliverable D1.2.3 (see http://tclouds-project.eu/);
M. Jensen, J. Schwenk, J.-M. Bohli, N. Gruschka, L. Lo Iacono (2011): *Security Prospects through Cloud Computing by Adopting Multiple Clouds*, Fourth IEEE International Conference on Cloud Computing, pp. 565-572.

TClouds
http://www.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/);
M. Jensen, J. Schwenk, J.-M. Bohli, N. Gruschka, L. Lo Iacono (2011): *Security Prospects through Cloud Computing by Adopting Multiple Clouds*, Fourth IEEE International Conference on Cloud Computing, pp. 565-572.

http://www.splitcloud.de/

Trustworthy Cloud: Secure Partitioning (1/2)

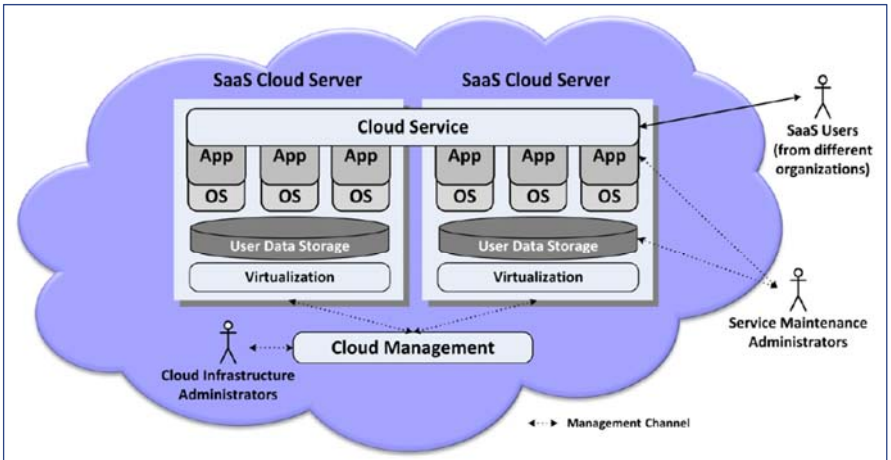


Fig. 1: SaaS-Cloud-Infrastructure architecture today: no isolation of users, user data and administrators

Deficiencies:

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

References:
A. Alkassar, M. Gröne, N. Schirmer (2015): *Secure Partitioning of Application Logic In a Trustworthy Cloud.* Proc. ISSE 2015, pp. 87-97.

http://www.splitcloud.de/

Trustworthy Cloud: Secure Partitioning (2/2)

Possible:

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

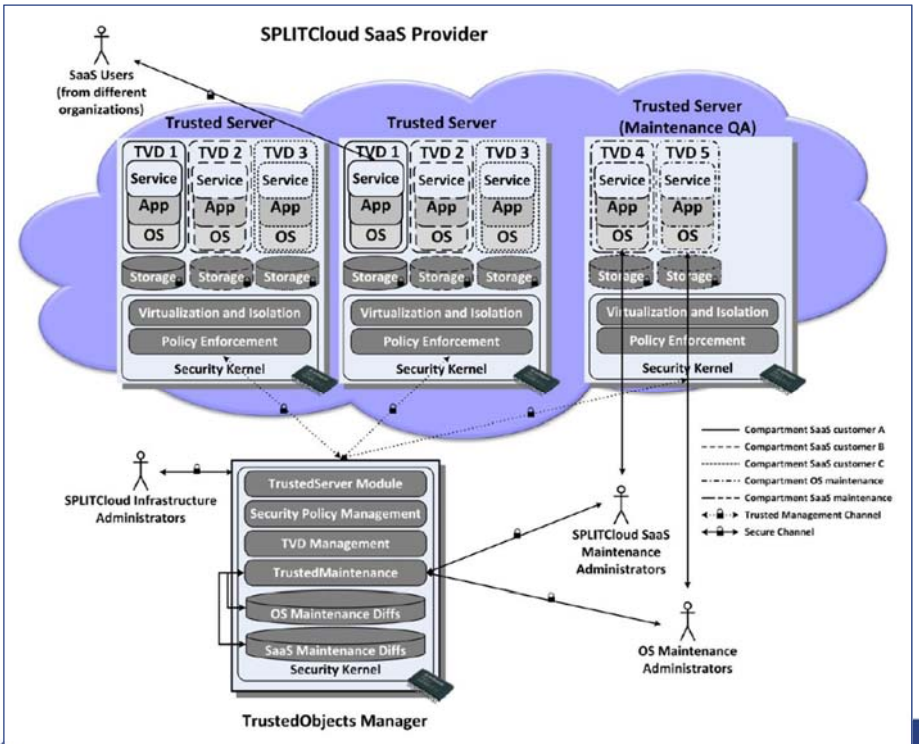


Fig. 2: SPLITCloud architecture – strict isolation and Service Maintenance without access to user data

References:
A. Alkassar, M. Gröne, N. Schirmer (2015): *Secure Partitioning of Application Logic In a Trustworthy Cloud.* Proc. ISSE 2015, pp. 87-97.

Combination with "Sealed Cloud"

- All application servers are in electromechanically sealed racks.
- The application servers dispose of volatile (clean-up area) memory only.
- Before internal staff or external spies can access a server, all unencrypted data is deleted irrevocably.
- The OS is additionally hardened and blocks all external access.

The OS reports status information from within yet accepts no orders from outside.

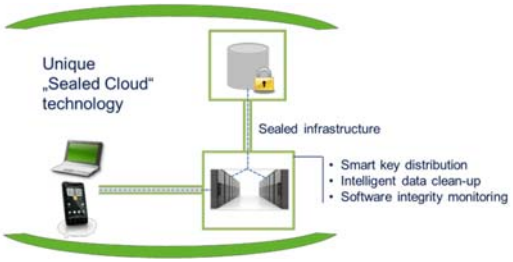
Result

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

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

Protection in the data centre:

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



Conclusion

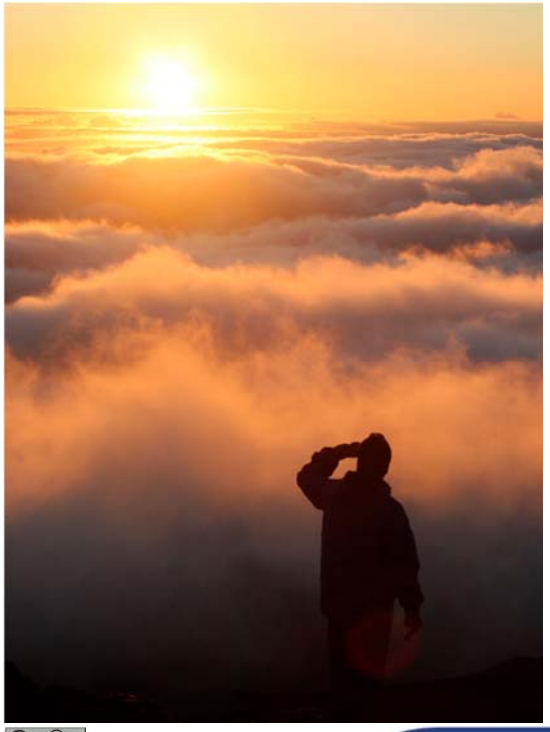


Photo: ewen and donabel

- 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/

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

References

- Standard Data Protection Model
  https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methodology_V1_EN1.pdf
- Art. 29 Working Party: Opinion 05/2012 on Cloud Computing
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
- Selection of Cloud projects
  - A4Cloud: www.a4cloud.eu/
  - TClouds: www.tclouds-project.eu/
  - SPLITCloud: www.splitcloud.de/
  - Sealed Cloud: www.sealedcloud.de/