Cloud Computing und Metadatenkonzepte

6. Darmstädter Informationsrechtstag

Life is for sharing.

Herausforderungen

Sicherheit / Data governance

Datenschutz

SLA / Abbildung von Geschäftsmodellen

Lock-in

Cloud administration

- Infrastructure clouds
  - Zugang durch den cloud – Anbieter, leaks?
- Platform clouds
  - Data governance in der Platform
  - Datenschutzkonformes handling
  - Gemeinsame Nutzung
- Application clouds
  - Hinreichende Datenschutz features
  - Lock - in

Fragen zu data governance

Zugriffsrechte und Administration

- Wer darf auf die Cloud zugreifen ?
- Wie erfolgt die Authentifizierung ?
- Wer administriert die Cloud ?

Speicherorte

- Wo werden die Daten gespeichert ?
- Kann der jeweils aktuelle Speicherort benannt werden ?
- Welche Maßnahmen des Zutrittschutzes sind getroffen ?

Data governance

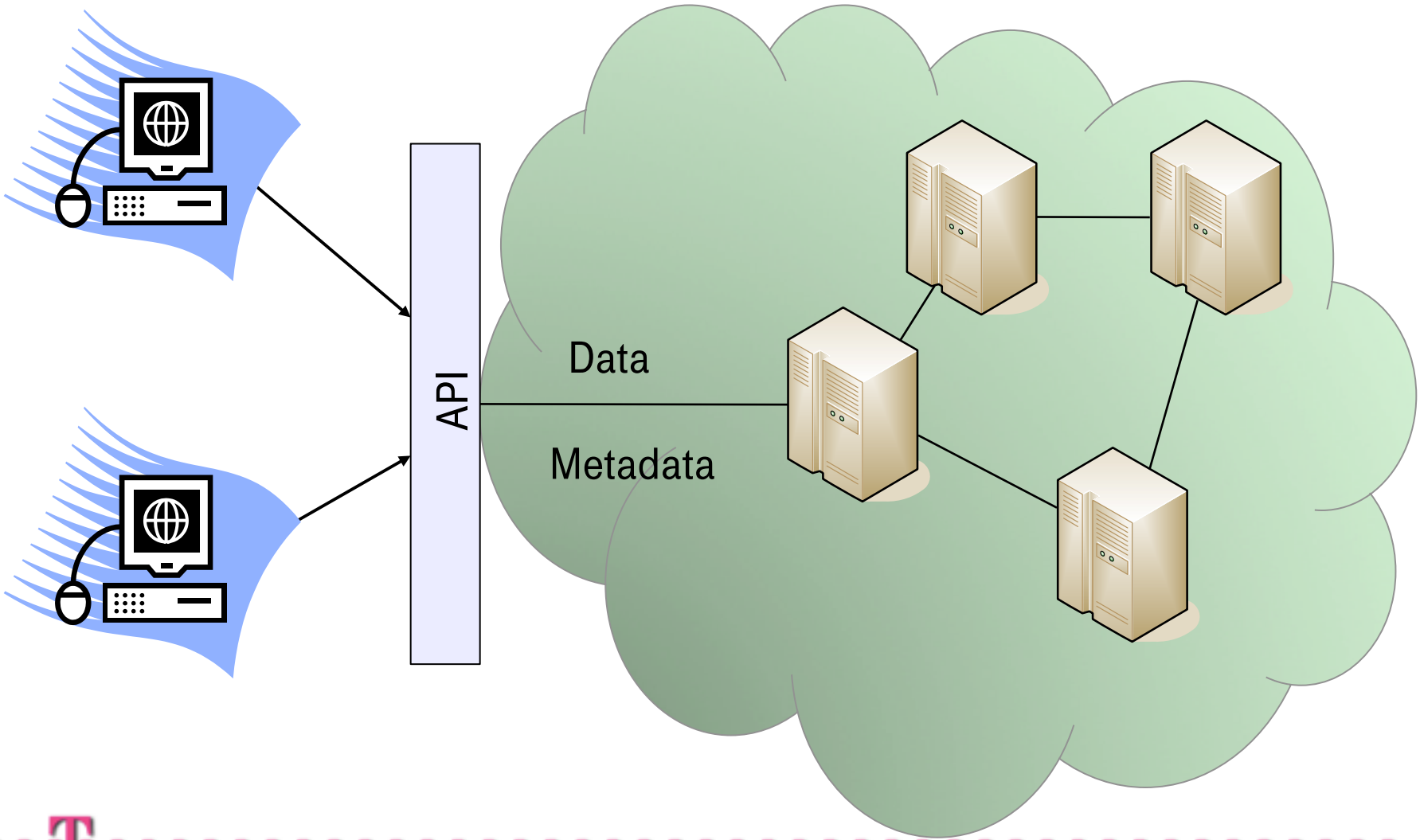
Cloud kann multiple Anbieter haben

- Transport der Verwendungsrestriktionen
- Policy Kombinationen (selektiv, kumulativ)
- Trigger und Pflichten (Information des Betroffenen)

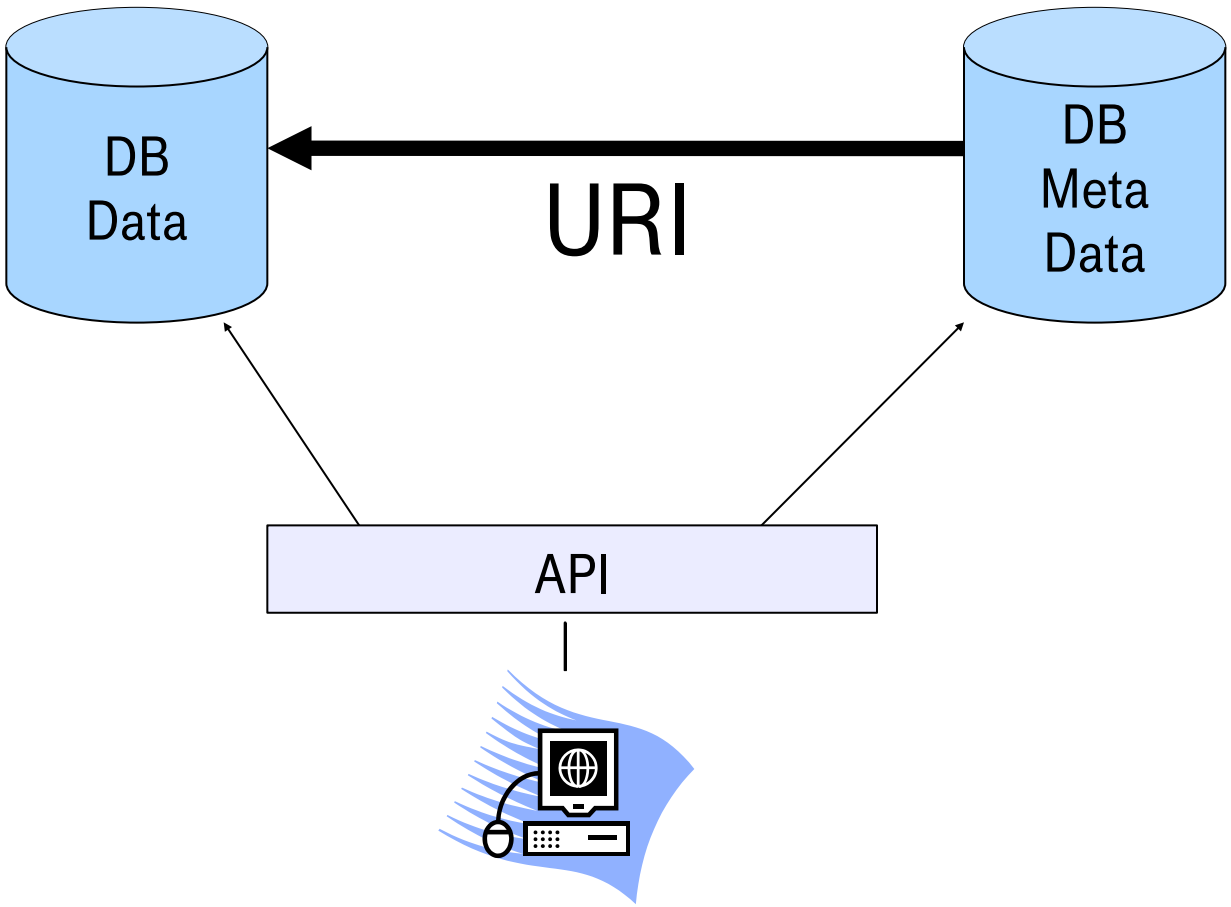
Cloud trägt nur einen Teil der Daten

- Datenschutzfördernde Teilung der Daten
- Analyse der Risiken
- Backup in verteilten Systemen

Data governance: How?

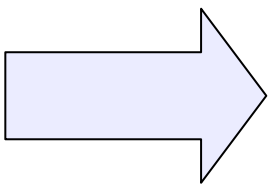


Data & Metadata



Governance by Metadata

- API muss Metadaten transportieren/kennen
- Cloud muss metadaten respektieren/kennen
- Governance transportierbar machen
  - XACML, SAML, WS-Policy, P3P, PrimeLife Obligations, SOAP, REST, etc....



Sticky Policy mit Governance Metadaten

Access control Unterstützung

- Cloud - Adressierbarkeit in XACML noch nicht unterstützt
- Neue Formen der Authentifizierung noch nicht interoperable (credential based)
- Verbot des Zugangs durch den cloud provider bisher nur juristisch (Versprechungen) Reicht das?
- Welche Semantiken der Zugangskontrolle werden in einer application-cloud unterstützt?

Anforderungen an SLA

Anforderungen an SLA aus datenschutzrechtlicher, deutscher Sicht:

- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Originalität
- Auditierbarkeit / Kontrollrechte

Auditierbarkeit von SLA bei public Clouds

Auditierbarkeit von SLA (exemplarisch):

- Amazon Web Service Customer Agreement
  http://aws.amazon.com/agreement/
  - „Wir bemühen uns, die Sicherheit Ihres Contents zu wahren, können dies jedoch nicht garantieren, da wir im Internet sind…“
  - „Sie sind verantwortlich für die Implementierung angemessener Sicherheitsmaßnahmen; Verschlüsselung sensitiver Daten eingeschlossen…“
  - Nur definierter Netzwerkverkehr ist zugelassen
  - Pen-Tests sind mit Einwilligung des Eigentümers der Applikation zugelassen

Auditierbarkeit von SLA bei public Clouds

- Google Apps Standardbestimmungen
  http://www.google.com/apps/intl/de/terms/standard_terms.html
  - Google hat ohne vorherige Ankündigung und ohne Haftbarkeit jederzeit (einschließlich der Betriebs- und Verfügbarkeitszeit jeder Servicefunktion) das Recht zum Ändern, Sperren oder Einstellen aller Teilbereiche des Services.
  - Der Kunde stimmt zu, dass er an keiner Aktion teilnimmt, die den Service oder mit dem Service verbundene Server oder Netzwerke stört oder unterbricht.
  - Google erlaubt Pen-Tests auf Applikationsebene gehosteter Apps

Sicherheit bei Clouds

- Auditunterstützung durch den Anbieter
  - Selbstverständlich ist es obligatorisch, sich beim Anbieter von der Wirksamkeit der getroffenen Maßnahmen zu überzeugen. Dies fordert auch der aktualisierte §11 BDSG.
  - Für “klassische” Betreiber von Rechenzentren normal, für Betreiber von Clouds wahrscheinlich eher ungewöhnlich.
- Langzeit-Verfügbarkeit der Services
  - Es bedarf gesonderter Festlegungen zum Umgang mit Situationen, wie z.B. Übernahme des Cloud-Anbieters durch ein größeres Unternehmen

Sicherheit bei Clouds

- Getrennte Verarbeitung
  - Wirksamkeit der getrennten Verarbeitung von unterschiedlichen Instanzen innerhalb der Cloud
  - Transparenz über die “anderen” Nutzer der Cloud
  - Transparenz über die “anderen” Nutzungen der Cloud
- Recovery
  - Wirksames Recovery beim Absturz der virtuellen Maschine
  - Wirksames Recovery beim Absturz der pysikalischen Maschine

Sicherheit bei Clouds

Netzwerksicherheit

- Anbindung an / Nutzung von Clouds über das Internet – verschlüsselte Verbindungen sind obligatorisch...
- SLA / EULA verbieten “ungewöhnlichen” Netzwerkverkehr
  - Manchmal wäre es sinnvoll, solchen Verkehr zu sehen
  - Werden Verstöße überwacht ?
- Penetrationstests in der Cloud
  - Bei salesforce.com und google für gehostete Applikationen zugelassen
  - Bei Amazon mit Einverständnis des Eigentümers der Applikationen zugelassen

Datenschutz bei Clouds

Gesetzeskonformität

- Wie vor jeder Verarbeitung ist zu Beginn die Zulässigkeit zu prüfen. Rechtsgrundlagen, Zweckbestimmung etc.
- Auskunfts- und eventuelle Beschlagnahmeregelungen anderer Länder sind bei internationalen Clouds unbedingt zu berücksichtigen.
- Ergeben sich aus den zu verarbeitenden Daten Restriktionen, die auf das Design der Public Cloud wirken ? (z.B. Daten nach TKG, SGB, KWG usw.)
- Rahmenbedingungen für On-, Near- oder Offshore (ADV, Safe Harbour oder Standard Contractual Clauses)

Weitere, bedeutsame Aspekte über den Datenschutz hinaus

- Security Aspekte werden in SLA abgebildet...
- Generelle Anforderungen
  - Verfügbarkeit
  - Integrität
  - Originalität
  - Auditierbarkeit / Kontrollrechte
- Forensik in der Cloud (bei fehlenden physikalischen Zugriffen...)

Weitere, bedeutsame Aspekte über den Datenschutz hinaus

- Business Continuity Planning
- Disaster Recovery
- Compliance Anforderungen
  - SOX
  - SAS 70
  - PCI
  - ... und weitere Anforderungen aus Gesetzen

Lock - in

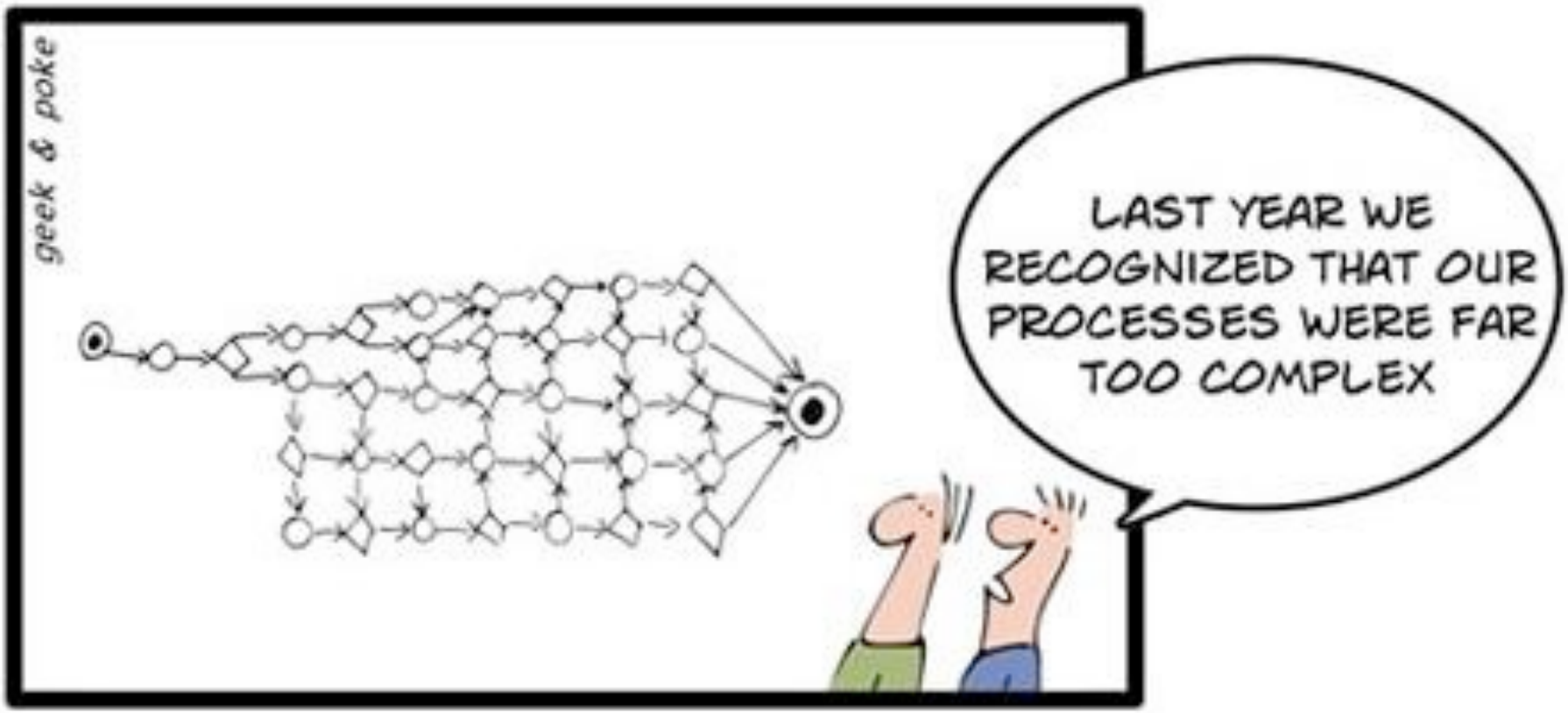
- Wie kommen meine Daten aus der cloud wieder heraus?
  - Standardisierte Formate für Platformen und Applikationen
- Bekomme ich meine metadaten wieder? z.B. Flickr
  - Standardisierte Metadaten - Formate
- Sind meine Geschäftsverbindungen an die cloud gebunden?
  - Identity management systeme (siehe Metadaten)

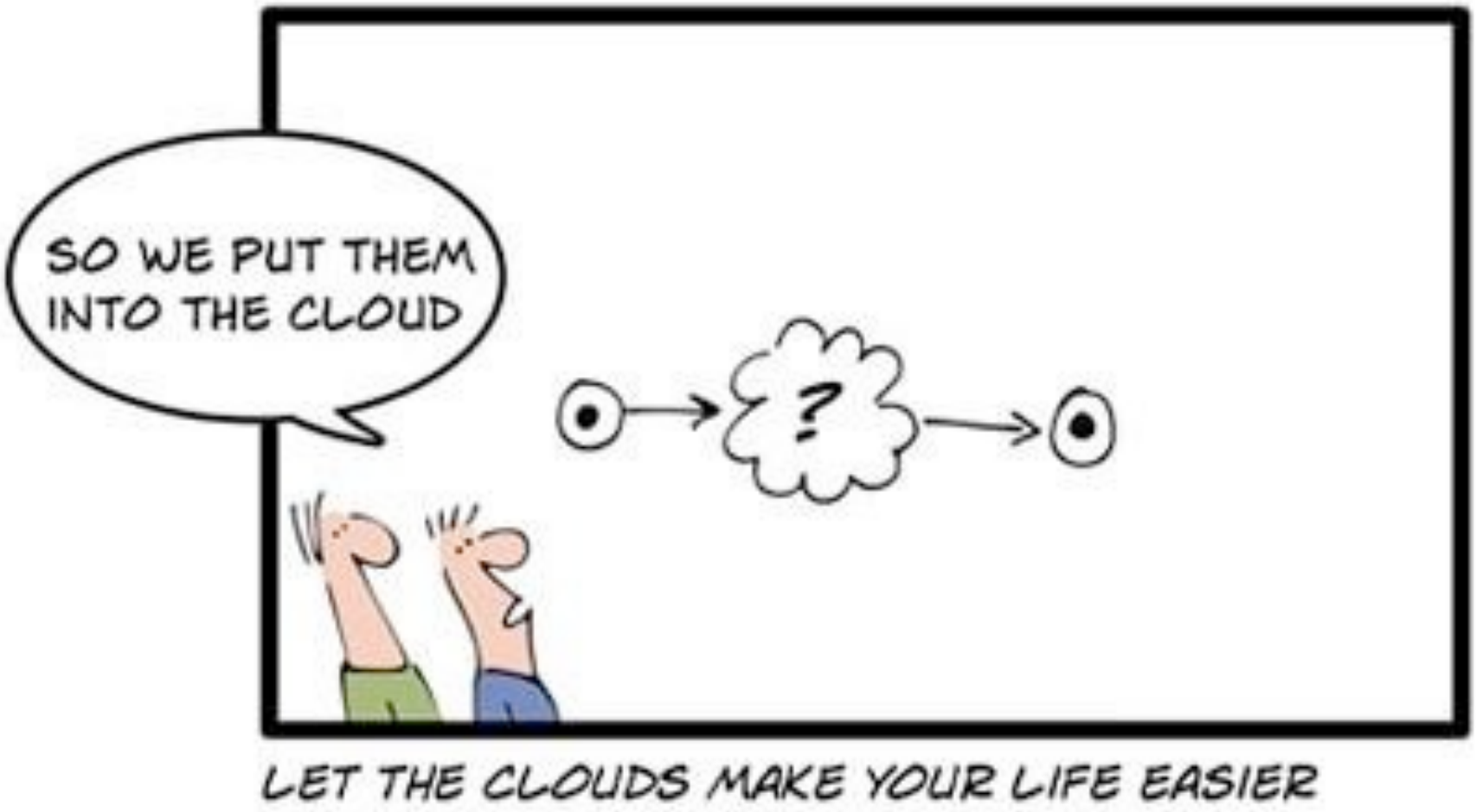
Leitfragen zur Beurteilung von Clouds

- Welches Deployment-Model liegt vor ?
  (public, private, hybrid Clouds)
- Welches Service Model liegt vor ?
- (IaaS, PaaS, SaaS)
- Wer managed / administriert die Cloud ?
- Wem gehört die Cloud ?
- Vertraue ich dem Anbieter der Cloud ?
  (und seinem Sicherheitsmodell?!)
- Wo befindet sich die Cloud ?
- Wer hat Zugriff auf die Cloud ?

Leitfragen zur Beurteilung von Clouds

- Wie wird die Cloud angesprochen ?
- Ist der Verlust der pysikalischen Kontrolle über die Ressourcen akzeptabel ?
- Unterstützt mich der Cloud-Anbieter bei Audits, Sicherheitsanalysen und ähnlichen Aktivitäten ?
- Wie erhalte ich Transparenz über:
  - Komposition der virtuellen Maschinen, Storage, Netzwerke ?
  - Datenflüsse, Speicherorte, Administration


geek & poke
LAST YEAR WE RECOGNIZED THAT OUR PROCESSES WERE FAR TOO COMPLEX


SO WE PUT THEM INTO THE CLOUD
?
LET THE CLOUDS MAKE YOUR LIFE EASIER

Fazit

Cloud computing ist:

- Datenschutzrechtlich unter bestimmten Bedingungen gestaltbar
  ➔ personenbezogene Daten in private clouds verarbeiten !
- Aus der Sicht des Datenschutzes technisch noch verbesserungsbedürftig
  ➔ eine Steuerung von Datenflüssen kann über Metadaten realisiert werden !
- Noch erfolgreicher, wenn die Art und Weise der Verarbeitung von Daten noch transparenter gemacht werden kann
  ➔ Metadatenkonzepte können die Transparenz von cloud computing erheblich steigern !

Thank you.

Frank Wagner

Senior Privacy Expert

Deutsche Telekom AG

Group Privacy

E-Mail: frank.wagner@telekom.de

Life is for sharing.