Trusted Cloud

Einführung

Gute Rahmenbedingungen für Cloud Computing: Recht und Datenschutz

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Die AG „Rechtsrahmen des Cloud Computing“

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Die Arbeitsgruppe "Rechtsrahmen des Cloud Computing"

- Teil des Kompetenzzentrums Trusted Cloud
- Leitung: Prof. Dr. Georg Borges
- Mitglieder der Arbeitsgruppe
  - Vertreter der Trusted Cloud-Projekte
  - externe Experten aus
    - Datenschutzbehörden
    - Verbänden
    - Cloud-Anbietern
    - Cloud-Nutzern
    - Rechtsanwaltschaft
    - Wissenschaft

Themenfelder und Aktivitäten

- **Urheberrecht**
  - Task Force „Vertrag und Lizenzen“
    Leitung: Dr. Marc Hilber, LL.M.
  - Arbeitspapier „Lizenzierungsbedarf beim Cloud Computing“ (2012)
  - Arbeitspapier „Cloud Computing und Open Source Software“ (2014)

- **Cloud Computing-Verträge**
  - Task Force „Vertrag und Lizenzen“
    Leitung: Dr. Marc Hilber, LL.M.
  - Leitfaden „Vertragsgestaltung beim Cloud Computing“ (2014)

Themenfelder und Aktivitäten

- **Datenschutz**
  - Task Force „Datenschutz“
    Leitung: Ulrich Lepper / Prof. Dr. Georg Borges
  - Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing “ (2012)

- **Haftung**
  - Task Force „Vertrag und Lizenzen“
    Leitung: Dr. Marc Hilber, LL.M.
  - in Bearbeitung: Leitfaden „Haftung und Cloud Computing“

Trusted Cloud

Themenfelder und Aktivitäten

- **Schweigepflicht / strafrechtlicher Geheimnisschutz**
  - Task Force „Geheimnisschutz“
    Leitung: Thomas Kranig
  - Thesenpapier „Schweigepflicht bei der Auslagerung von IT-Dienstleistungen“ (2015)

Trusted Cloud

Gute Verträge für Cloud Computing

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Es diskutieren

- **Dr. Marc Hilber, LL.M.**, Oppenhoff & Partner
- **Peter Niehues**, regioIT
- **Stephan Sädtler**, Universität Passau


Trusted Cloud
Kompetenzzentrum Trusted Cloud
Leitfaden –
Vertragsgestaltung
beim Cloud Computing
Nr. 3

Leitfaden – Vertragsgestaltung beim Cloud Computing

- Erstellt von der AG Rechtsrahmen des Cloud Computing
- 25 Seiten Zusammenfassung der wichtigsten Themen
- Einschließlich umfassender Checkliste
- Neutral (berücksichtigt sowohl Anbieter- als auch Kundensicht)
- Relevante Punkte anreißen, Problembewusstsein schaffen

Interessenlage beim Cloud Computing

- Die Sicht der Kunden
  - Compliance
  - Kosten

- Die Sicht des Anbieters
  - Umsetzung von innovativen, flexiblen Geschäftsmodellen
  - Leistungsbeschreibung/Festlegung im SLA
  - Nutzungsende/Kündigung

Inhalt des Leitfadens

- Anwendbares Recht und Gerichtsstand
- Vertragsgestaltung und Vertragstypologie
- Leistungsbeschreibung und Change Management
- Service Level Agreements
- Kündigung und Exit

Haftungsaspekte beim Cloud Computing

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Es diskutieren

- **Dr. Alexander Duisberg**, Bird & Bird LLP
- **Alexander Glaus**, Deutsche Bank AG
- **Dr. Marc Hilber**, Oppenhoff & Partner

Haftungsaspekte beim Cloud Computing

- Haftung des Cloud-Anbieters für die eigene Leistung
- Haftung für Datenverluste
- Vertragliche Haftungsbeschränkungen
- Haftung für rechtswidrige Inhalte
- Haftung des Cloud-Nutzers

Trusted Cloud

Reformen im Rechtsrahmen: Geheimnisschutz

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Es diskutieren

- **Thomas Kranig**, Bayerisches Landesamt für Datenschutzaufsicht
- **Dr. Joseph Walenta**, Deutsches Herzzentrum Berlin


Trusted Cloud
Kompetenzzentrum Trusted Cloud
Thesenpapier – Schweigepflicht bei der Auslagerung von IT-Dienstleistungen
Nr. 7

Datenschutz und § 203 StGB

- Einsatz externer IT-Dienstleister durch Berufsgeheimnisträger
- bei Ausgestaltung als Auftragsdatenverarbeitung datenschutzrechtlich zulässig
- „Offenbaren" jedoch strafbar (§ 203 StGB)
- Strafbarkeitsrisiko bei Nutzung von Cloud-Diensten

Das Papier der AG Rechtsrahmen

- de lege lata kein rechtssicherer Einsatz von Cloud Computing durch Berufsgeheimnisträger möglich

- Möglichkeiten der Reformierung
  - Änderung des Gehilfenbegriffs
  - Änderung des BDSG
  - Änderung der Berufsordnungen
  - Konkretisierung des Offenbarungsbegriffs

Erfordernis der Gesetzesänderung

- zwangsläufiges Strafbarkeitsrisiko
- Referentenentwurf zum E-Health-Gesetz ignoriert die Problematik
- Rechtsklarheit durch einheitliche gesetzliche Lösung
- Favorisiert: Konkretisierung des Offenbarungsbegriffs in § 203 StGB

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

- November 2013 – April 2015
- Leitung: Prof. Dr. Georg Borges
- Projektbeteiligte
  - 7 Datenschutzbehörden
  - 3 Verbände
  - 4 Cloud-Anbieter
  - 2 Rechtsanwaltssozietäten
  - 2 Anbieter von IT-Prüfungen
  - DIN
  - Stiftung Datenschutz

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

- Beobachterstatus
  - Europäische Kommission
  - Bundesministerium des Innern
  - Bundesamt für Sicherheit in der Informationstechnik

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

- Ziel: Erarbeitung der Grundlagen einer Datenschutz-Zertifizierung

- Grundlage: Konzept der AG Rechtsrahmen des Cloud Computing (Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“)

- Im Einzelnen:
  - Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)
  - Konzepte zu zentralen Aspekten der Zertifizierung
  - Untersuchungen zum Verfahren der datenschutzrechtlichen Zertifizierung

Veröffentlichungen

- Arbeitspapier „Modulare Zertifizierung von Cloud-Diensten“ (2014)
- Thesenpapier „Datenschutz-Zertifizierung durch private Stellen“ (2015)
- Arbeitspapier „Vertikaler Aufbau von Cloud-Diensten“ (Veröffentlichung als Entwurf, 2015)

In Bearbeitung:

- Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“
- Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)
- Arbeitspapier „Aspekte des datenschutzrechtlichen Zertifizierungsverfahrens“

Die Datenschutz-Grundverordnung – Stand des Gesetzgebungsverfahrens und Ausblick

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

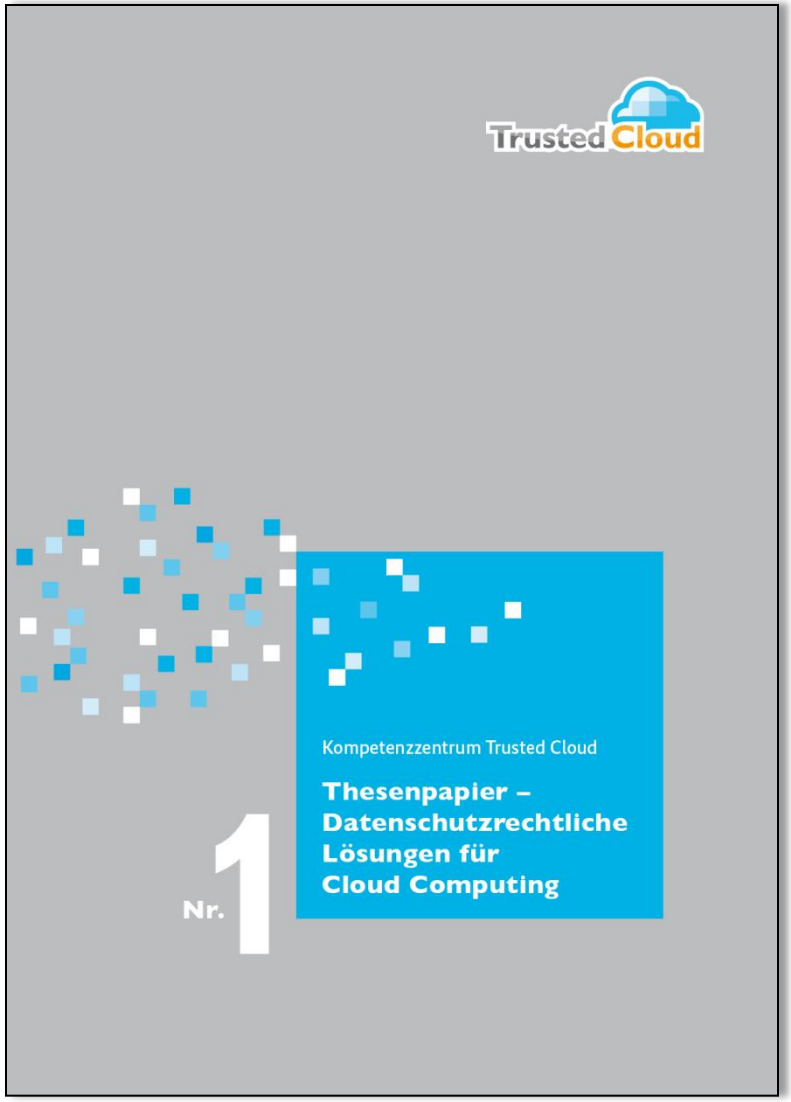
Trusted Cloud

Datenschutz-Zertifizierung durch private Stellen

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Es diskutieren

- **Thomas Kranig**, Bayerisches Landesamt für Datenschutzaufsicht
- **Monika Wojtowicz**, TÜViT GmbH
- **Dr. Claus Ulmer**, Deutsche Telekom AG


Trusted Cloud
Kompetenzzentrum Trusted Cloud
Thesenpapier –
Datenschutzrechtliche
Lösungen für
Cloud Computing
Nr. 1

Trusted Cloud

These 8

Das Testat sollte (auch) durch qualifizierte private Stellen vergeben werden. Die Eignung der testierenden Stelle sollte durch eine Akkreditierung nachgewiesen werden. Die testierende Stelle sollte für fehlerhafte Testate haften.

Trusted Cloud

Anforderungen an Zertifizierer aus Sicht der Praxis

- Zertifizierungen müssen verlässlich sein
- Rechtssicherheit durch einheitliche Anforderungen
- Angemessene Balance zwischen staatlichen und privaten Stellen
  - Entwicklung der Prüfanforderungen durch private Stellen
  - Überprüfung der Prüfanforderungen durch staatliche Stellen
  - Akkreditierung durch staatliche Stellen
  - Zertifizierung durch private und staatliche Stellen
- Zertifizierungsmodelle müssen praktisch anwendbar sein

Das Angebot an Zertifizierern

- Anbieter von Zertifizierungen im Datenschutz
  - Deutschland: 31 *(Zertifizierungsübersicht der Stiftung Datenschutz, 2014)*
  - EU: 13 *(Studie zu Datenschutzsiegeln im Auftrag der EU-Kommission, 2013)*

- Private Stellen mit behördlicher Anerkennung
  - De-Mail-Datenschutznachweis (BfDI)
  - Datenschutz-Gütesiegel (ULD)

Trusted Cloud

Sicht der Datenschutzaufsicht

- Entscheidung über Einhaltung der datenschutzrechtlichen Anforderungen ist primär Aufgabe der Aufsichtsbehörden

- Zertifizierung ist auch durch private Stellen denkbar, wenn Aufsichtsbehörden eingebunden sind bei
  - Akkreditierung der privaten Zertifizierungsstellen
  - Festlegung der Prüfanforderungen

Die Datenschutz-Grundverordnung

- Art. 39 Abs. 1d DSGVO-E (Europäisches Parlament)
  „1d. […] Die endgültige Zertifizierung erteilt die Aufsichtsbehörde."

- Art. 39a Abs. 1 DSGVO-E (Entwurf der ital. Ratspräsidentschaft)
  „Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 wird die Zertifizierung von einer Zertifizierungsstelle erteilt, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt. Jeder Mitgliedstaat teilt mit, ob diese Zertifizierungsstelle akkreditiert wurde von […]"


Trusted Cloud
Kompetenzzentrum Trusted Cloud
Thesenpapier – Datenschutz-Zertifizierung durch private Stellen
Nr. 6

Trusted Cloud

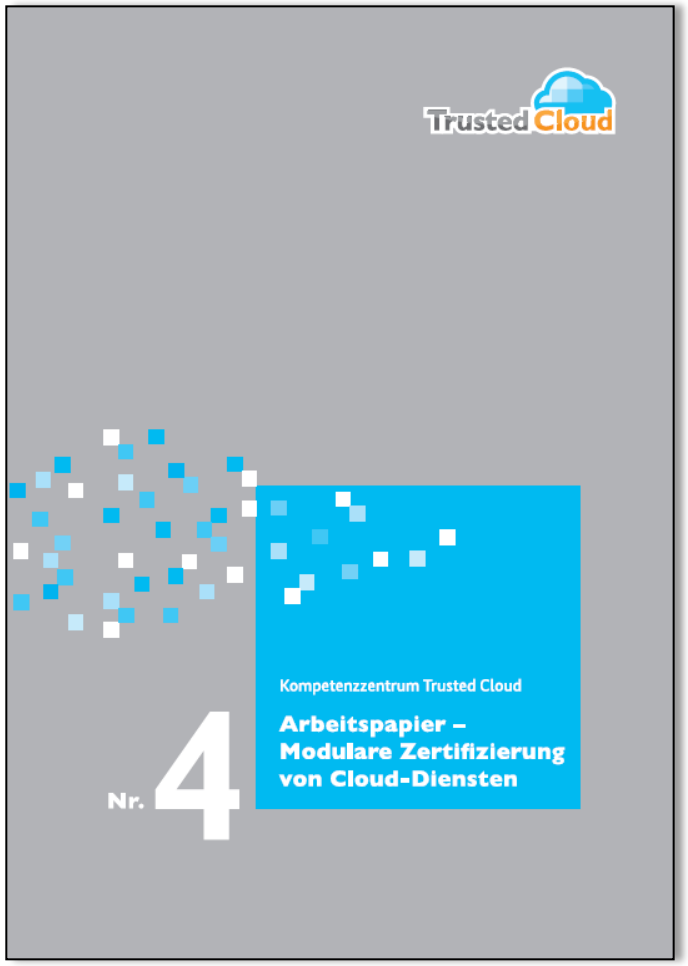
Prüfanforderungen für Cloud-Dienste

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

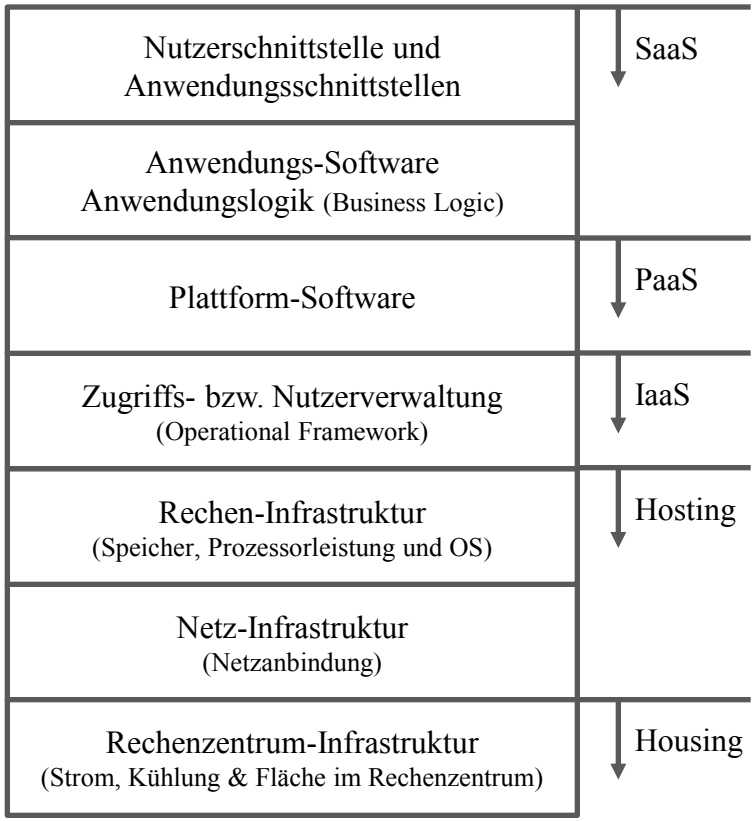
Es diskutieren

- **Mathias Cellarius**, SAP SE
- **Dr. Hubert Jäger**, Uniscon universal identity control GmbH

Effizienz durch modulare Zertifizierung



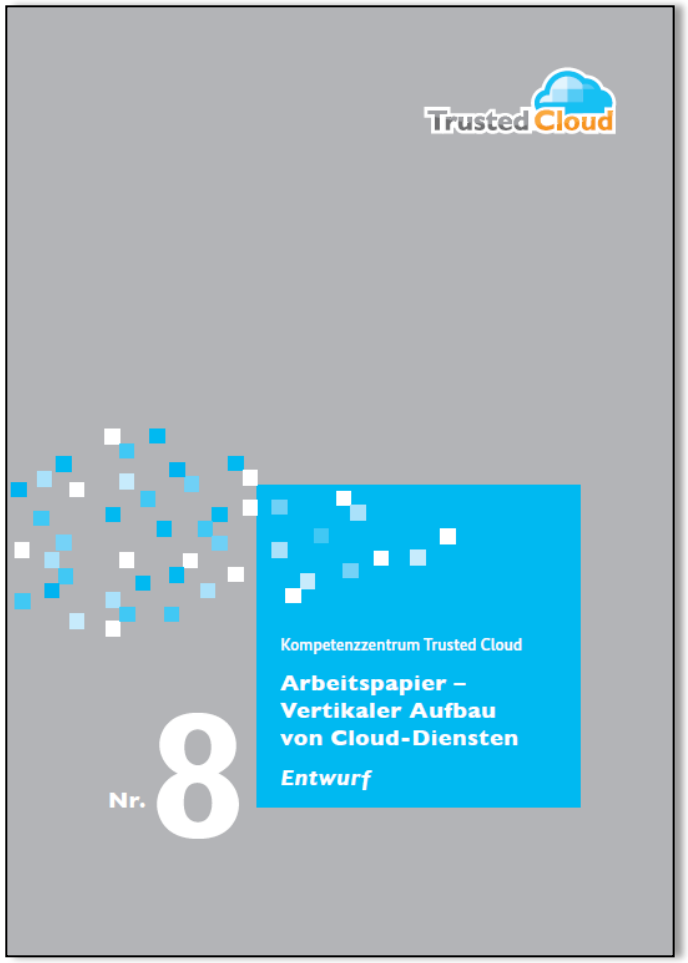
Der modulare Aufbau von Cloud-Diensten



Der modulare Aufbau von Cloud-Diensten

SaaS	Nutzerschnittstelle und Anwendungsschnittstellen	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen
	Anwendungs-Software Anwendungslogik (Business Logic)	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen
PaaS	Plattform-Software	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen
IaaS	Zugriffs- bzw. Nutzerverwaltung (Operational Framework)	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen
Hosting	Rechen-Infrastruktur (Speicher, Prozessorleistung und OS)	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen
	Netz-Infrastrukttur (Netzanbindung)	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen
Housing	Rechenzentrum-Infrastruktur (Strom, Kühlung & Fläche im Rechenzentrum)	Nutzer-Schicht Zugriffs-Schicht Dienste-Schicht Ressourcen-Schicht	Integration	Datensicherheit	Datenschutz	Betriebs-Unterstützung	Geschäfts-Unterstützung	Entwicklungs- und Einsatz-Unterstützung	Organisatorische Grundlagen

Der modulare Aufbau von Cloud-Diensten



Das Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)

- Grundlage: BDSG

- ISO/IEC 27018 „Information technology — Security techniques — Code of practice for PII protection in public clouds acting as PII processors” (2014)

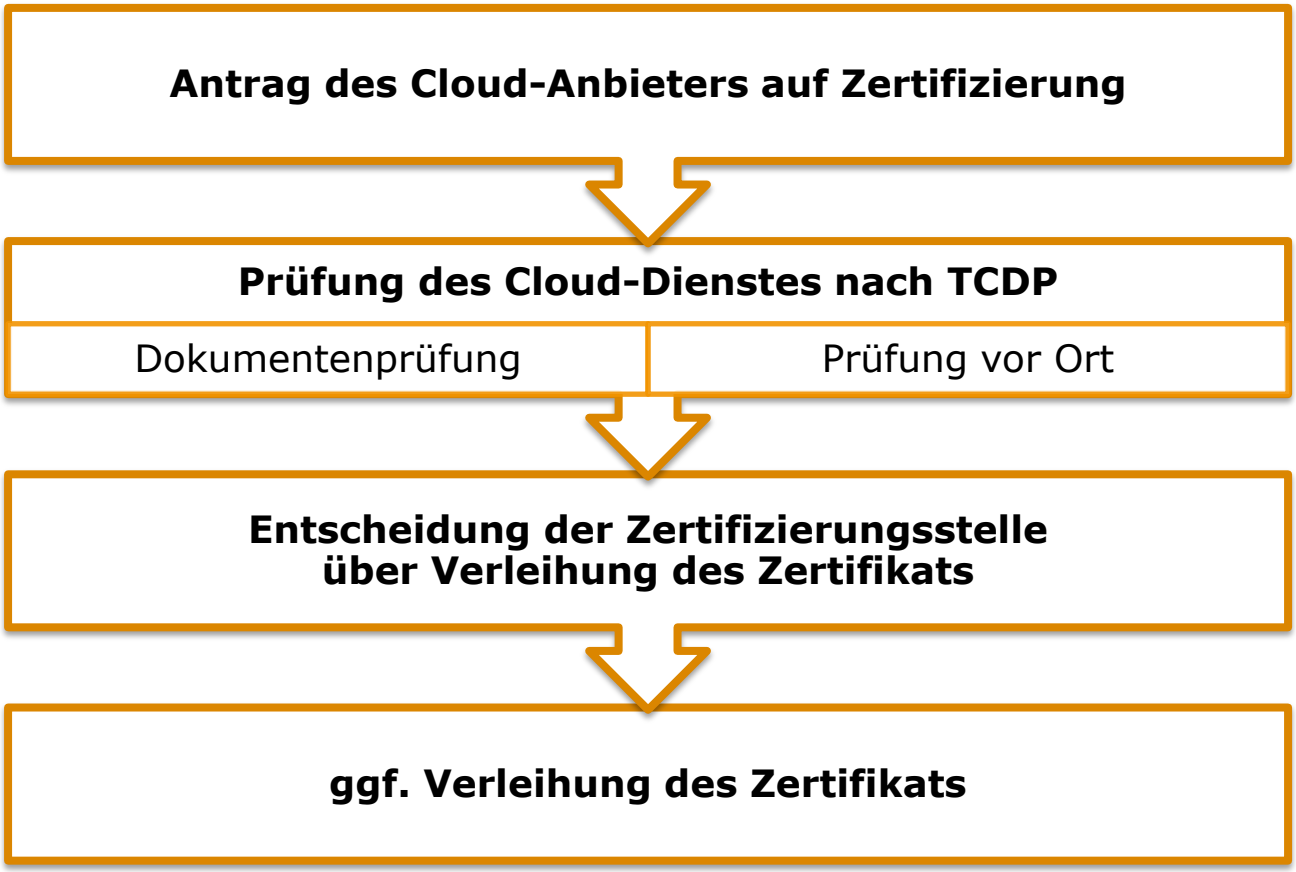
Das Zertifizierungs-verfahren

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Es diskutieren

- **Thomas Doms**, TÜV Trust IT
- **Frederick Richter**, Stiftung Datenschutz
- **Karin Vedder**, Bayerisches Landesamt für Datenschutzaufsicht

Der Weg zum Datenschutzzertifikat



Unabhängigkeit und Eignung der Stelle

- Akzeptanz von Zertifikaten setzt Vertrauen voraus
- Voraussetzung: Eignung und Unabhängigkeit der Zertifizierungsstellen
- Qualitätssicherung durch Akkreditierung der Zertifizierungsstellen

Aussage und Rücknahme des Zertifikats

- Aussage des Zertifikats:
  - Dienst erfüllt die datenschutzrechtlichen Anforderungen
  - Zertifikate üblicherweise auf 3 Jahre befristet

- Rücknahme des Zertifikates
  - wenn Voraussetzungen entfallen oder nie vorlagen
  - Veröffentlichung der Rücknahme wie bei Zertifikatserteilung

Haftung für Fehler bei der Zertifizierung

- Hohe Relevanz der Haftung
- Verantwortlichkeit der Zertifizierungsstelle für ordnungsgemäßen Ablauf des Verfahrens Art. 39a Abs. 4 DSGVO-E
- Problem: Prüfung ist zeitpunktbezogen
- Erforderlich: aktiver Prozess bei Veränderungen und Meldeprozess bei Fehlern für Servicenutzer

Trusted Cloud

Die Zukunft der Zertifizierung von Cloud-Diensten

Trusted-Cloud-Abschlusskonferenz
Berlin, 11. Februar 2015

Die Zukunft der Zertifizierung von Cloud-Diensten

- Der Rechtsrahmen für Cloud Computing
  Abschlussveranstaltung AG Rechtsrahmen des Cloud-Computing / Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“
  Berlin, 13. April 2015

- Projekt „Praktische Umsetzung der Datenschutz-Zertifizierung für Cloud-Dienste“