Cloud und Compliance

Dr. iur. Cyrill Rieder
Rechtsanwalt & Partner bei Fuhrer Marbach & Partner
www.fmp-law.ch
rieder@fmp-law.ch

Experts Live Switzerland

Session Übersicht

1. Compliance: Was heisst das für die Cloud?
2. Vertraulichkeit: Dürfen Geheimnisse in die Cloud?
3. Datenschutz: Was gilt bei Personendaten?
4. Exkurs: Der US Cloud Act: Was steht da drin?
5. Take Aways & Fragen

1. Was ist Compliance in der Cloud?

Die Compliance beschreibt die Regeltreue eines Unternehmens

Umsetzung und Überwachung gesetzlicher, regulatorischer und freiwilliger Vorgaben

Vermeidung von Streitigkeiten

Wem gehören Daten und Informationen?

- **Grundsatz:** Kein Eigentum an Daten. Wer Daten hat kann sie verwenden

- **Ausnahme:** Nutzung wird von Gesetz oder Vertrag beschränkt

Doch der Ausnahmen sind viele…

- Regulatorische Schranken
- Datenschutzrechtliche Schranken
- Wettbewerbsrechtliche Schranken
- Lauterkeitsrechtliche Schranken
- Immaterialgüterrechtliche Schranken
- Vertraglich vereinbarte Schranken

Keine einheitliche Rechtslage für die Cloud:

- Staat des Cloudnutzers, des Betreibers, des Kunden oder des Konsumenten

- Spezialgesetze für einzelne Unternehmen

- Produkt- oder Branchenstandards

- Technologiespezifische Regeln

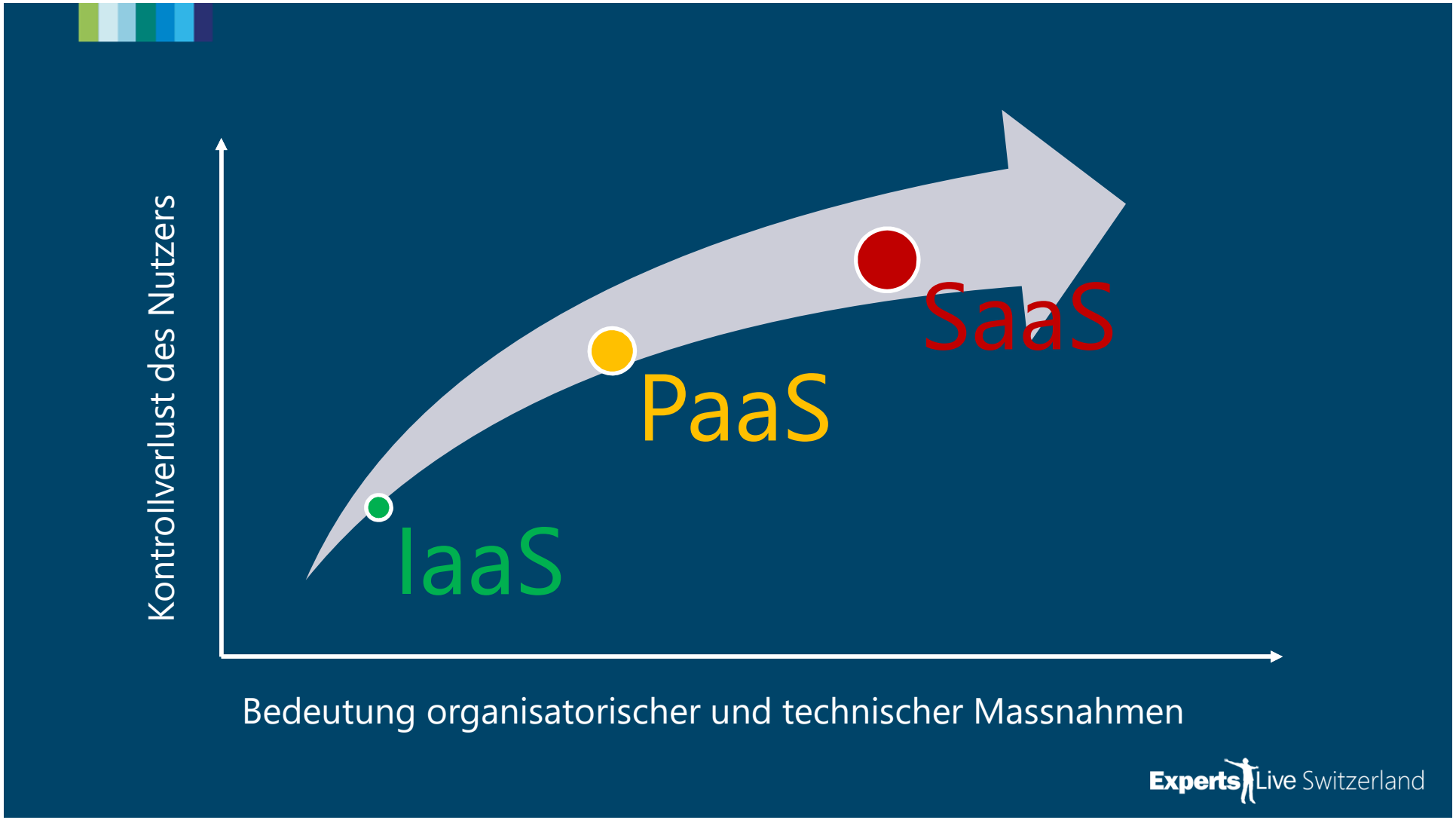
Kontrollverlust bei Cloud Services:

- physischer Perimeter: Infrastrukturzugang
- logischer Perimeter: techn. Schutzmechanismen
- personeller Perimeter: Interne Abläufe
- zeitlicher Perimeter: Geschäftspolitik

Gegenüber dem Gesetzgeber
bleibt der Cloud Nutzer
vollumfänglich verantwortlich!

⇒ Organisatorische und technische Massnahmen (sog. TOMs)

⇒ Vertragliche Regelungen


Kontrollverlust des Nutzers
IaaS
PaaS
SaaS
Bedeutung organisatorischer und technischer Massnahmen
Experts Live Switzerland

Compliance erfordert im Einzelfall :

- Abgrenzung der Risikosphären
- Berücksichtigung des regulatorischen Umfelds
- Bestimmung der rechtlichen Anforderungen
- Transparente Kommunikation im Projekt
- Technische & organisatorische Massnahmen
- Dokumentation und Protokollierung
- Audit und Kontrollmassnahmen

2. Vertraulichkeitsverpflichtungen

- Gesetzliches Berufs- oder Amtsgeheimnis
  - Anwälte und Notare
  - Ärzte und Gesundheitspersonal
  - Banken und Versicherungen
  - Beamte und Amtsträger
- Geheimhaltungsvereinbarungen

=> Haftungsrisiken, Konventionalstrafen, Bussen und Freiheitsstrafen

Keine Offenbarung bei:

- pseudonymisierten Daten

- aggregierten Daten oder anonymisierten Daten

- Verschlüsselten Daten

Weitergabe von Geheimnissen an Cloud Anbieter:

- Es liegt keine unzulässige Offenbarung vor 
- Gesetzliche Haftung des Geheimnisträgers 
- Sorgfaltspflichten hinsichtlich Auswahl, Instruktion & Überwachung des Anbieters 
- Zugriffsrechte von Aufsichtsorganen 

=> Einwilligung des Geheimnisherrn 

Der Geheimnisträger muss zur Gewährleistung der Geheimhaltung alles «Zumutbare» unternehmen:

- Eignung des Cloudanbieters
- Verpflichtung zur Geheimhaltung
- Sicherheitsdispositiv mit Schutzmassnahmen
- Begrenzung des Personenkreises
- Evaluierung & Sensibilität der Daten
- Inländische vs. ausländische Cloud-Provider

3. Datenschutz in der Cloud

Das Datenschutzrecht regelt das Bearbeiten von Daten, über bestimmte oder bestimmbare Personen.

- Es geht um Informationen über Personen (Tatsachen/Werturteile)
- Es geht um den Schutz der Persönlichkeit (sog. informationelle Selbstbestimmung)

Die Datenschutzgesetze schützen Personendaten:

- unzulässigen „Verarbeitung“
- Qualität und Integrität der Daten
- Verfügbarkeit der Daten im Bedarfsfall

Schutzniveau variiert je nach Staat
=> Compliance Risiken

Zulässigkeit von Datenbearbeitungen: Verarbeitung von Personendaten ohne Rechtfertigung unzulässig:

- Vorliegen einer Einwilligung
- Vertragserfüllung, wenn Betroffener Vertragspartei
- Erfüllung einer rechtlichen Verpflichtung
- Lebenswichtige Interessen des Betroffenen
- Aufgabe im öffentlichen Interesse
- Wahrung berechtigter Interessen

Weitergabe von Personendaten an Cloud Anbieter:

- Information der betroffenen Personen
- Einwilligung bei sensible Personendaten
- Vertrag: Cloudanbieter darf die Daten nur so verwenden, wie der Cloud Nutzer es darf
- Cloud Nutzer haftet für Einhaltung des Datenschutzrechts.
- Vertragliche Datenschutzgarantien bei Übertragung ins Ausland

Einwilligung: Sog. «informed consent»:

- Freiwilligkeit
- Klare und einfache Sprache
- Information über konkrete Datenbearbeitung
- Information über Widerrufsrecht
- Einwilligung mit aktiver eindeutiger Handlung
- Nachweisbarkeit der Einwilligung

4. Exkurs: Der US Cloud Act

- Speicherort von Daten ist zufällig und wechselt
- Behörden kommen nur schwer an ausländische Daten (Multi Legal Assistance Treaties)
- Staaten haben ev. legitimes Interesse andere Staaten am Zugriff auf Daten zu hindern
- USA erhalten viele Rechtshilfeanfragen, da Cloud Provider ihren Sitz in den USA haben

- Entscheidender Gerichtsfall: Microsoft v. US, 829 F.3d 197 (2nd Cir. 2016) => Supreme Court
- Zugriff der US Behörden auf im Ausland gespeicherte Daten von US Bürger
- Limitierter Schutz für Personen anderer Nationalität ohne Aufenthalt in USA
- Abschluss von Cloud Act Agreements, wenn Rechtssysteme gleichwertigen Rechtsschutz bieten.

- Unbekannte Personen üben in UK ein Verbrechen aus und koordinieren über einen Cloud Service.

- Die UK Strafverfolgungsbehörden wollen Zugriff auf Daten des Providers. Nach UK Recht müssen die Daten herausgegeben werden.

- Providersitz in USA: Herausgabe nach US Recht nur in Verfahren nach US Recht zulässig (MLAT).

=> Cloud Agreement: USA verhindert/sanktioniert die Datenherausgabe nach UK Recht nicht.

5. Take Aways & Fragen

- Für die Cloud gelten vielseitige und unkoordinierte Regelungen
  => Widersprüche sind die Folge!
- Die Compliance Verantwortung verbleibt beim Cloudnutzer
  => Organisatorische und Technische Massnahmen!
- Rechtliche, organisatorische und technische Risikobeurteilung
  => Einzelfallbetrachtung der betroffenen Daten!
- Auswahl, Instruktion und Überwachung des Anbieters
  => Kontrolle ist Pflicht!
- Reduktion von Compliance Risiken
  => Verschlüsseln, Anonymisieren und Pseudonymisieren!

Noch Fragen?

Herzlichen Dank für
Ihre Aufmerksamkeit!

Sponsoren


Hewlett Packard Enterprise
digicomp
isolutions
SYNTARO
WE DO IT LIGHT
pohn
unconditionally Cloud
au2mator
make it noble
Microsoft
SmartIT
Adfinis SyGroup
audiocodes
Experts Live Switzerland