Darf ich das?

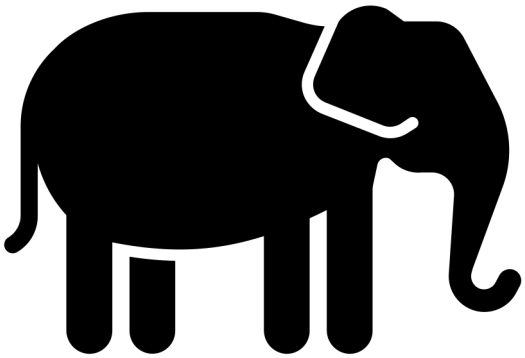
Aktuelle Richtlinien und Ratschläge wie man mit seinen Daten in der Cloud umgeht

Dr. Christian Laux
Rechtsanwalt, LL.M. (Stanford)

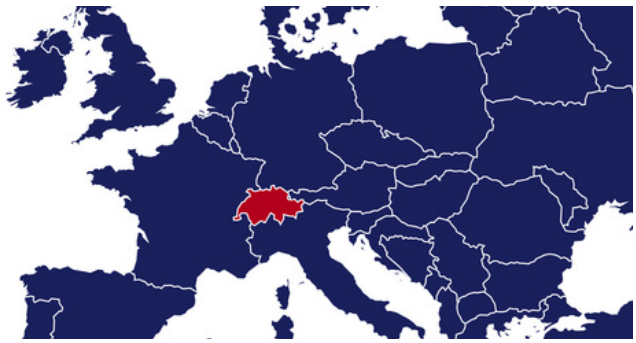
LAUX LAWYERS AG
ZURICH | BASEL

Super WebGate Day
Gottlieb Duttweiler Institut
23. Mai 2019

LAUX LAWYERS AG
ZURICH | BASEL



Was bedeutet der Standort Schweiz?



Was heisst «Datenschutz»?

Das Datenschutzgesetz («DSG») verlangt im Allgemeinen:

- die Einhaltung von gewissen Verfahren
- Beschränkungen in der Datennutzung
- eine besondere Organisation

Das DSG regelt den Personendatenschutz.

Was heisst «Datenschutz»?

Was ist «Datenschutz» sonst noch?

- Zugang
- Verwertung
- Löschung

nach Strafrecht, Wettbewerbsrecht, Immaterialgüterrecht und Vertragsrecht

ausserdem: Regulierung (nur wenige Branchen)

Was heisst «Datenschutz»?

Schliesslich: Ein Entscheid des Nutzers

- Manchmal strategisch
- Auf jeden Fall intern
- Nicht immer rational begründbar

Verantwortung > Kontrolle

LAUX LAWYERS AG
ZURICH | BASEL

- Jeder ist verantwortlich für sein eigenes Verhalten
  → Kunde behält die Verantwortung
- Nachweis ordnungsgemässer Geschäftsführung?
  → Kontrolle
- Arbeitsteilige Wirtschaft
  → „Kontrollverlust“ (ist normal oder scheinbar)
- Warum die Frage nach dem Kontrollverlust?
  → Dritteinflüsse
- Oft hört man: „Kunde ist ja selber leichtsinnig bezüglich Daten“
  → nicht relevant (andere Vertragsbeziehung!)

Problem

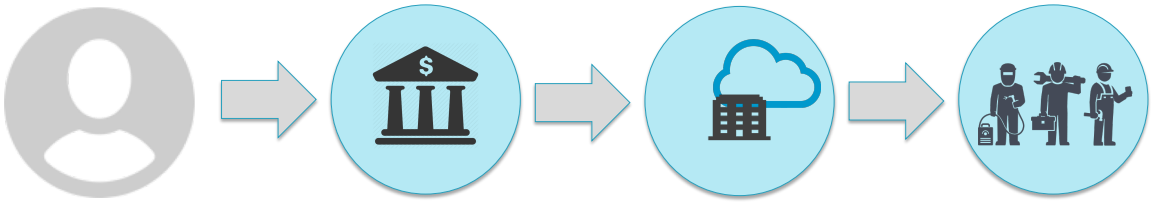
Ohne Offenbarung keine Haftung

LAUX LAWYERS AG
ZURICH | BASEL

Was bedeutet „Offenbarung“?

„**Klartext-Zugriff**“ ist der relevante Begriff

Methode: **Technisch-rechtliche Analyse**



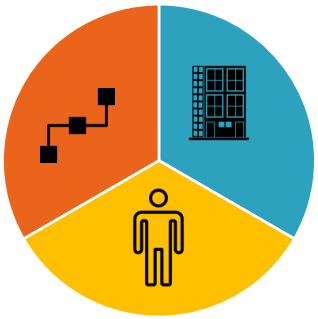
Kunde (z.B. Bank) **Cloud-Anbieter** **Sub-Akkordanten**

Kontrolle

Perimeter: Geheimnisschutz heisst Perimeterschutz

Perimeterbegriff ist weiterhin von Bedeutung

Perimeterbegriff ist der Einstieg zur Definition von “Kontrolle”



Aber: Der Fokus auf Daten wird wichtiger. → **Datenklassifizierung**.

9

Cloud-Gutachten für Banken

LAUX LAWYERS AG
ZURICH | BASEL

- Cloud-Leitfaden der SBVg:
  - https://www.swissbanking.org/library/richtlinien/cloud-leitfaden-wegweiser-fuer-sicheres-cloud-banking
- Rechtsgutachten LLAG:
  - https://www.swissbanking.org/library/richtlinien/rechtsgutachten
  - https://www.lauxlawyers.ch/en/rechtsgutachten-bankgeheimnis-und-cloud

Banken: Strengste Branche

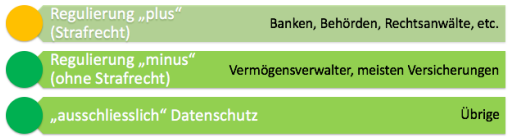
- nur wenige andere Branchen kennen so strenge Geheimnispflichten
- nur wenige Branchen haben ähnlich strenge Aufsicht

Cloud Landschaft

Interpretationshinweis: Dies ist kein roter Knopf!

Regulierung „plus“ (Strafrecht)	Banken, Behörden, Rechtsanwälte, etc.
Regulierung „minus“ (ohne Strafrecht)	Vermögensverwalter, meisten Versicherungen
„ausschliesslich“ Datenschutz	Übrige

Anforderungen



Kundengruppe	Datenschutz	Aufsicht	Geheimhaltung
Oberer Bereich: Bankenwesen (im Besonderen)	**Zwingend**	**Zwingend**	**Zwingend**
Mittlerer Bereich: Versicherungen (im Besonderen)	**Zwingend**	**Zwingend**	Nicht relevant
Unterer Bereich: “gewöhnliche Industrie“	**Zwingend**	Nicht relevant	Nicht relevant

Mantras

LAUX LAWYERS AG
ZURICH | BASEL

- Kontrollieren kann nur, wer auch versteht
- Die Antwort liegt in der Technik (es gibt kein Voodoo)
- Themenführerschaft beanspruchen

Massnahmen > Kontrolle

LAUX LAWYERS AG ZURICH | BASEL

- Technische Massnahmen
- Organisatorische Massnahmen
- Vertragliche Massnahmen

Wer entscheidet und wer beeinflusst den Entscheid?

LAUX LAWYERS AG ZURICH | BASEL

- „Unteres Band“: Management
- „Mittleres Band“: Management „plus“
  - Sachversicherung: FINMA
  - Lebensversicherung: FINMA
  - Krankenversicherung: FINMA + BAG
  - Unfallversicherung: FINMA + BAG
  - Asset Management: Revisionsstelle („langer Arm“)
- „Oberes Band“: Management „plus“
  - Banken: Revisionsstelle
  - Behörden und Anwälte: Behörde / Kanzlei selber

Wer entscheidet und wer beeinflusst den Entscheid?

- Datenschutzgesetz («DSG»)
- Fragestellungen:
  - Zustimmung („Consent“)
  - Informationspflicht („Notice“)
    - Spannend: Intuitiv → warum nicht?
    - Tatsächlich: sinnvoll?
- Unterschied „normale“ Personendaten v. „besonders schützenswerte“ Personendaten?
  - Im Behördenumfeld: Ja (nach DSG)
  - Sonst: nicht cloud-relevant

Standards

- Technische und organisatorische Massnahmen
- „FINMA-zertifiziert“ gibt es nicht
- Das Recht legt unterschiedliche Standards an:
  - DSG: Angemessenheit
  - Strafrecht: Zustimmung nötig wenn „Offenbarung“
- Bei Angemessenheits-Prüfschwelle:
  - Effektive Kontrollen
  - Standards zur Vereinfachung der Planung
  - Standards zur Vereinfachung des Nachweises

Welche Regelwerke?

LAUX LAWYERS AG
ZURICH | BASEL

Planende Sicht

- ISO 27001 für Infrastrukturen
- ISO 27017 (Security, Shared Roles, Hardening Virtual Machines)
- ISO 27018 (Informationsschutz)
- eventuell: ISO 20000 für managed services
- auch andere Modelle, z.B Cobit mit Fokus Planung

Welche Regelwerke?

LAUX LAWYERS AG
ZURICH | BASEL

Prüfende Sicht

- ISAE 3000 / ISAE 3402 (Typ 1, Typ 2)
- SOC 1 / SOC 2
- Lokale Adaptationen (US: SSAE 18, DE: IDW PS)
- Wichtig:
  - Braucht Anker im Cloud-Vertrag
  - Z.B. Amendments für Finanzwirtschaft

Best Practices (1/4)

- Analysetiefe hängt ab von:
  - Management Buy-in
  - Strittigkeit der Rechtsfragen

Best Practices (2/4)

- Public Only oder Hybrid?
- Transparenz des Dienstleisters (siehe auch Folgeslide)
  - Due Diligence
  - Abstützen auf Dokumente: OK
  - Voraussetzung: Internes Know How
- Monitoring Veränderungen
  - Konnex zu interner Governance-Organisation

Best Practices (3/4)

Transparenz vom Provider einfordern

Drei-Kreise-Modell

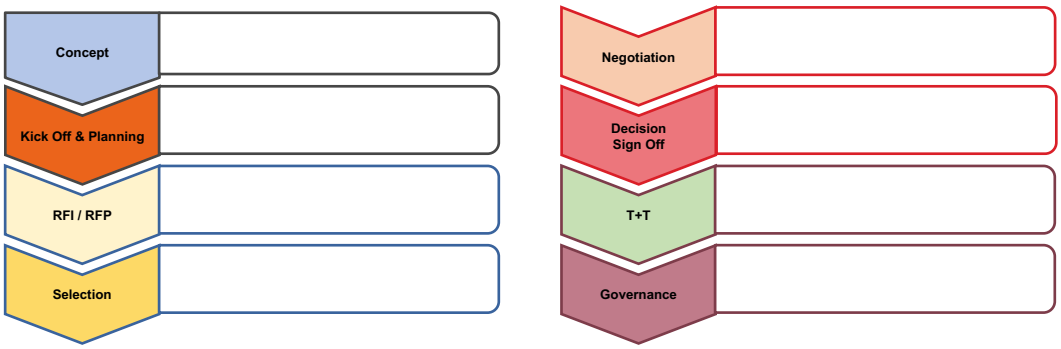
1) Äusserer Kreis: Öffentlich verfügbare Information (Whitepapers, etc.)
2) Mittlerer Kreis: Ergänzende Darstellungen und Erläuterungen auf Anfrage durch dediziertes technisches Personal
3) Innerer Kreis: Konkrete IT-Fragen («Aufzeigen der eigentlichen Innereien»)

Best Practices (4/4)

- Prüfrechte:
  - Abstützen auf Drittprüfer: OK
  - Voraussetzung: Definition der Standards und Einsicht
- Besonders schützenswerte Personendaten
  - In der Schweiz?
  - Auch im Ausland möglich.

Beratungsframework

Wir beraten auf der Basis des von uns entwickelten Werkzeugkastens:



Kontakt

Dr. Christian Laux
Rechtsanwalt
christian.laux@lauxlawyers.ch

LAUX LAWYERS AG
http://www.lauxlawyers.ch

Seegartenstrasse 2
Postfach 360
CH – 8024 Zurich
+41 44 880 24 24