Cloud Computing aus datenschutzrechtlicher Sicht

Dr. iur. Barbara Widmer LL.M.,
CIA (Certified Internal Auditor)

15. Juni 2018

Schweizer Anwaltstag 2018 in Schaffhausen

Marc Zuckerberg:

«Einst lebten wir auf dem Land, dann in Städten und jetzt im Netz».

Referatsinhalt

I. Grundlagen Cloud Computing

II. Rechtlicher Rahmen

III. Auftragsdatenbearbeitung nach CH-DSG und EU-Datenschutzgesetzgebung

IV. Trends

V. Fazit

I. Grundlagen

Was ist Cloud Computing?

Anbieten von

- **Rechenleistung**,
- **Speicherplatz**,
- **Software**

als **Dienstleistung über Internet** ⇨ via Web-browser

I. Grundlagen

Was ist Cloud Computing?

Merkmale:

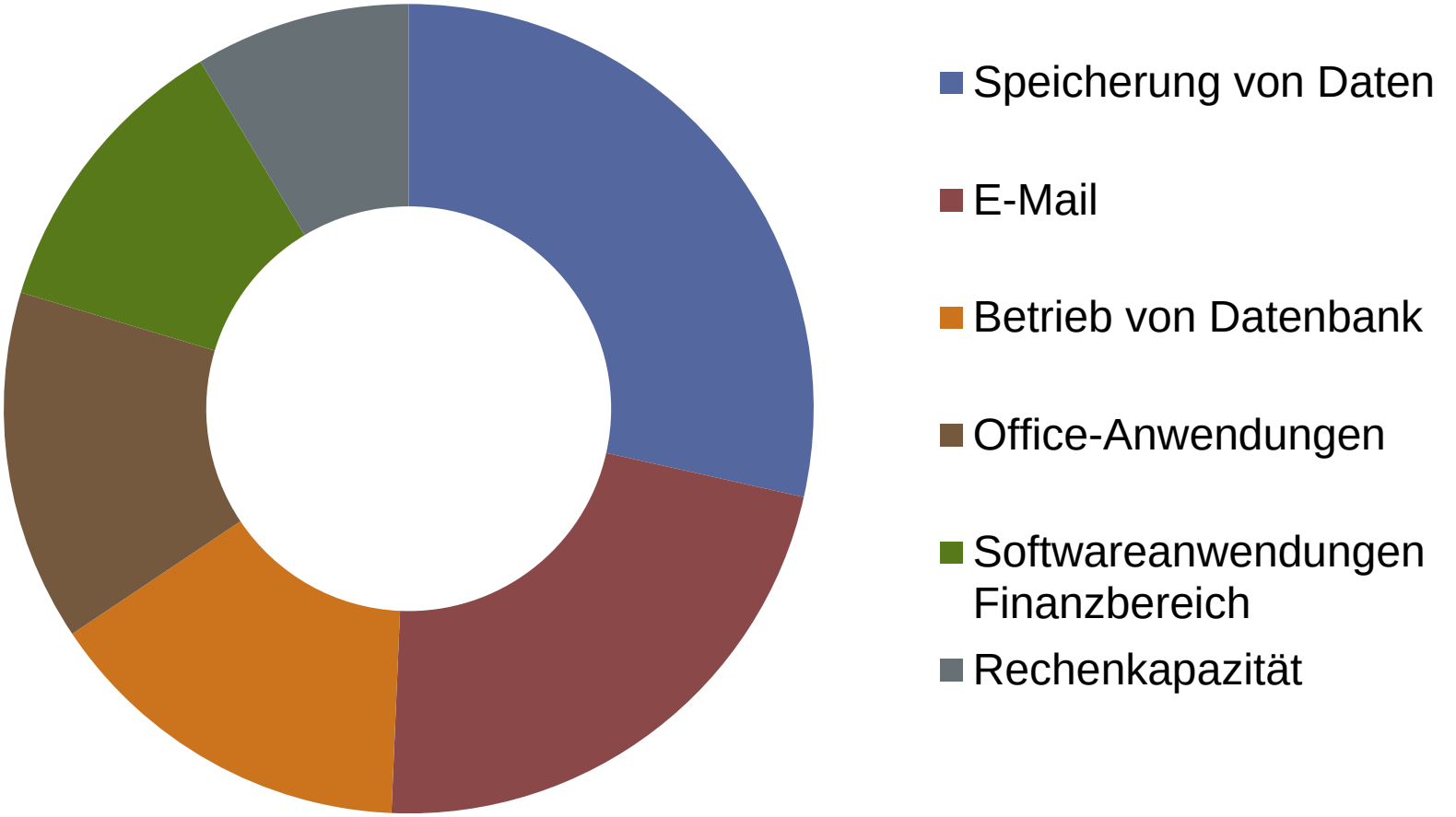
- **bedarfsgerechte** Verfügbarkeit,
- **verbrauchsabhängige** Verrechnung

der **Leistungen**

⇨ hohe **Flexibilität** und **Kosteneffizienz**

I. Grundlagen

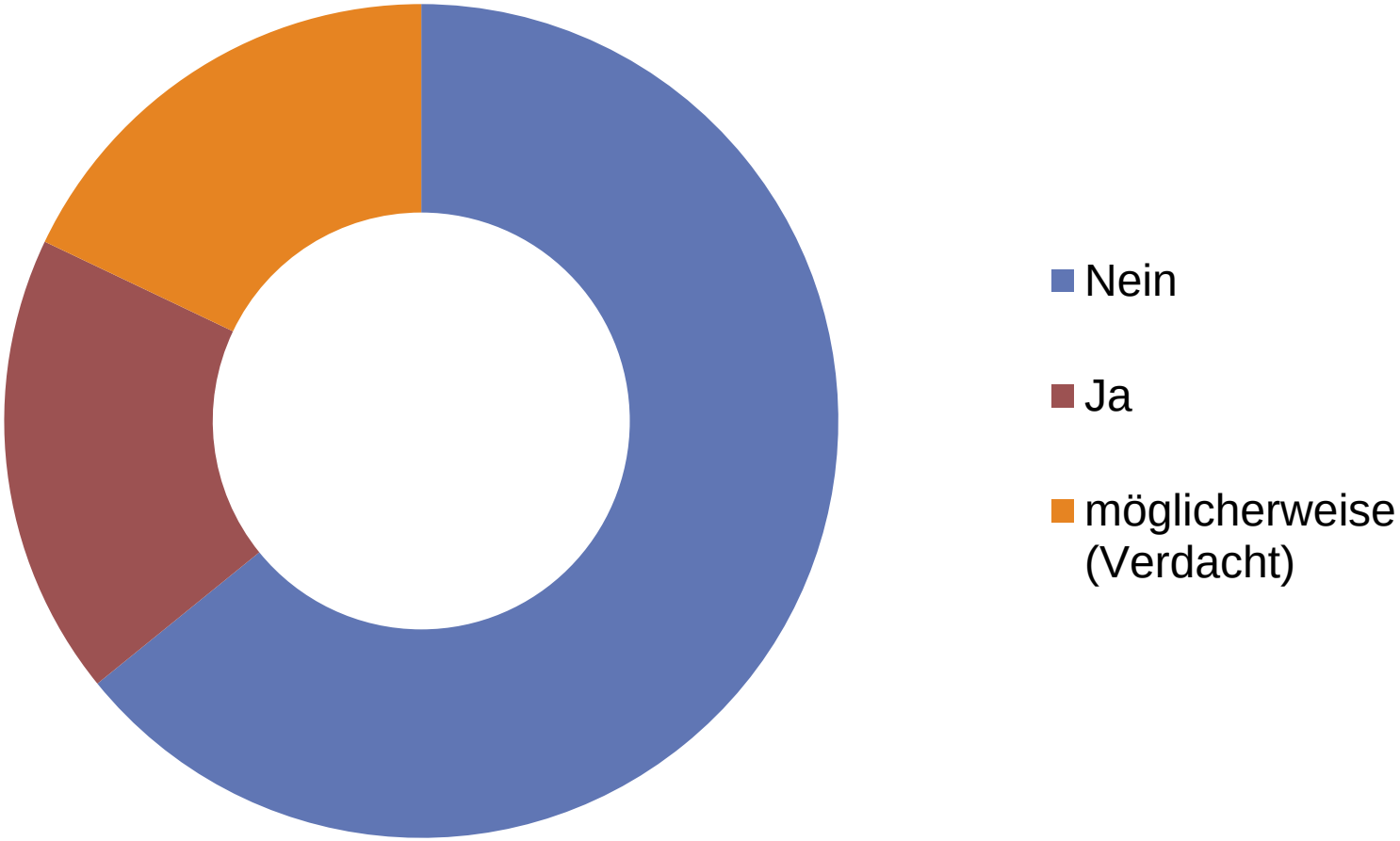
Nutzungsverhalten 2016 (deutsche Unternehmen)



Quelle: Statista.com

I. Grundlagen

Sicherheitsvorfälle 2016 (deutsche Unternehmen)



Quelle: Statista.com

II. Rechtlicher Rahmen

Cloud Anbieter **bearbeitet Daten** des Cloud Nutzers durch

- Betrieb Softwareapplikationen
- zur Verfügung stellen von Speicherplatz und Infrastruktur

⇨ Bearbeitung umfasst regelmässig **personen-bezogene Daten**

= **Datenschutzgesetzgebung** anwendbar.

II. Rechtlicher Rahmen

Datenschutzrechtliche Qualifikation:

Beauftragung von Dritten mit Datenbearbeitung

= Auftragsdatenbearbeitung

Rechtsgrundlagen:

Art. 10a DSG bzw. Art. 8 E-DSG

III. Auftragsdatenbearbeitung

Rechtsgrundlage

Art. 10a DSG:

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn

a. Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfe.

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

[2] …

Art. 8 E-DSG:

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsverarbeiter übertragen werden, wenn

a. Die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] …

[3] …

III. Auftragsdatenbearbeitung
lit. a – wie Auftraggeber selbst

Wie Auftraggeber Daten selbst bearbeiten darf ergibt sich aus

- anwendbarer **Datenschutzgesetzgebung**
- anwendbaren **spezialgesetzlichen Vorgaben**

III. Auftragsdatenbearbeitung
lit. a – wie Auftraggeber selbst

Erfüllung von lit. a setzt voraus:

1. **Ermittlung** massgeblicher Regelungen
2. **Überbindung** deren Inhalte mittels Vertrag auf Auftragnehmer
   - ⇨ mittels eigenständiger Datenschutzvereinbarung oder als Teil des Dienstleistungsvertrags
3. **Einhaltungsüberprüfung** durch Auftrag-geber

III. Auftragsdatenbearbeitung
lit. a – wie Auftraggeber selbst

Umsetzung der **Punkte 2 und 3 bei Cloud Computing** nicht einfach:

- oft **internationaler** Sachverhalt – Kollisionen,
- **Marktmacht** des Anbieters – wenig Verhand-lungsspielraum,
- Daten auf **mehrere Server** verteilt und/oder **Serverstandorte** unbekannt.

III. Auftragsdatenbearbeitung
lit. b - Geheimhaltungspflicht

Gesetzlich oder vertraglich:

- **gesetzlich** – z.B. Amtsgeheimnis, Berufsgeheimnisse, Fernmeldegeheimnis
- **vertraglich** – vertraglich vereinbarte Geheimhaltungspflichten

III. Auftragsdatenbearbeitung
lit. b - Geheimhaltungspflicht

…**ABER, Einzelfallprüfung** – zielt Geheimnis darauf ab, konkret zur Diskussion stehende Auftragsdatenbearbeitung zu verhindern?

…**NEIN -** Geheimnis steht Auslagerung aus **datenschutzrechtlicher Sicht** nicht entgegen,

…**ABER,** Geheimhaltungspflicht Drittem voll-umfänglich überbinden.

III. Auftragsdatenverarbeitung

EU-Datenschutzgesetzgebung

Nicht zum Lesen…

Artikel 28

Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen —, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

III. Auftragsdatenverarbeitung
EU-Datenschutzgesetzgebung

Art. 28 DSGVO (Auftragsverarbeiter)

Abs. 1:

Auftraggeber muss sicherstellen, dass Auftragsverarbeiter hinreichende Garantien bietet […], dass

- Verarbeitung in Einklang mit Anforderungen dieser Verordnung erfolgt und
- Schutz der Rechte der betroffenen Personen gewährleistet ist.

III. Auftragsdatenverarbeitung
EU-Datenschutzgesetzgebung

Abs. 2:

Untervertragsverhältnisse ⇨ schriftliche Genehmigung durch Auftraggeber

Abs. 3:

Inhaltsvorgaben vertragliche Vereinbarung zwischen Auftraggeber und Auftragnehmer

Abs. 10:

Auftragsverarbeiter fallen unter Bussgeldregelung der EU-Datenschutzgesetzgebung

III. Auftragsdatenverarbeitung
EU-Datenschutzgesetzgebung

Art. 3 Abs. 1 DSGVO (Räumlicher Anwendungsbereich)

EU-Datenschutzgesetzgebung ist auf **in EU niedergelassene Auftragsverarbeiter** anwendbar - auch wenn

- **Verarbeitung** nicht in EU stattfindet
- **Auftraggeber** sich nicht in EU befindet.

⇨ **Kollision mit CH-Regelung - will CH-Recht auf Auftragsverarbeiter anwenden.**

III. Auftragsdatenverarbeitung
EU-Datenschutzgesetzgebung

Unterschiede zu CH Regelung:

- **keine Geheimhaltungspflicht** als mögliches Auslagerungshindernis,
- **Untervertragsverhältnis** nur mit schriftlicher **Einwilligung** (gesetzlich vorgegeben),
- **Auftragsdatenverarbeiter** in EU untersteht **EU-Datenschutzgesetzgebung**

III. Auftragsdatenverarbeitung
Auftragnehmer mit Sitz im Ausland

…ist möglich, Auftragnehmer muss Daten jedoch nach CH-Recht bearbeiten – egal wo er sich befindet ⇨ Kollision mit EU-Recht

UND Auftraggeber muss sorgfältige **Risiko-analyse** durchführen ⇨ **massgebend** sind

- Sensitivität der Daten,

- Datenschutzsensitivität im Auslagerungsland.

III. Auftragsdatenbearbeitung
Risikoanalyse

Sensitivität der Daten - Vertragsgestaltung:

Daten	Server-standort	Unter-vertrag	Anwendbares Recht	Gerichts-stand
heikle Daten	CH	nein	CH	CH
eher heikle Daten	CH/EU-MG	eher nein	CH/EU-MG	CH/EU-MG
wenig heikle Daten	offen	offen	offen	offen

III. Auftragsdatenbearbeitung
Risikoanalyse

Datenschutzsensitivität – Wahl Auslagerungsland:

Land	Anwendbares nationales Recht	Datenschutzsensitivität
EU	EU-Datenschutzgesetz-gebung (DSGVO)	hoch, jedoch nicht in allen MG gleich
USA	- US-Recht, - Privacy Shield CH-USA	es kommt darauf an…
Russland, China, Indien usw.	jeweilige nationale Gesetzgebung	niedrig bis inexistent

IV. Trends

Quo vadis Cloud Computing?

⇨ **Zunahme und Weiterentwicklung**

⇨ **Treiber** sind:

- Globalisierung
- vermehrte Nutzung mobiler Endgeräte (iPhone, Tablets, Laptops usw.)
- Kostendruck in IT-Bereich
- Verbesserung Wettbewerbsfähigkeit

V. Fazit

Cloud Computing

- wird kaum aufhaltbar sein
- ist an sich gute Sache
- Datenschutz verhindert Cloud Computing nicht, setzt aber Leitplanken
- Auftraggeber ist verantwortlich, dass Auftragnehmer Datenschutzvorgaben einhält

Vielen Dank für Ihre Aufmerksamkeit!