SF·FS

# 3. DATENSCHUTZRECHTSTAGUNG

## Datenschutz in Bewegung

29. Mai 2019, 13:45 – 18:00 Uhr

Universität Zürich, Raum RAA-G-01

Rämistrasse 59, 8001 Zürich

Mit Spannung wurden die ersten Bussen zur DSGVO erwartet. Auch wenn naturgemäss vieles offen bleibt, legt sich der Staub allmählich, und erste Fragen wurden beantwortet, etwa zum Anwendungsbereich der DSGVO. Auch in der Schweiz hat sich einiges bewegt; zwar weniger bei der Revision des DSG, wohl aber in der Fallpraxis des EDÖB. Der erste Teil der Tagung bringt auf den neusten Stand über wichtige Entwicklungen der letzten zwölf Monate in der EU und in der Schweiz und bietet ausreichend Raum für Fragen und Diskussionen im Rahmen einer Panel- und Plenumsdiskussion. Hier erfährt der Praktiker, was die Aufsichtsbehörden hüben wie drüben erwarten.

Im zweiten Teil der Tagung werden in drei Referaten und einer weiteren Panel- und Plenumsdiskussion einige besonders aktuelle Fragen vertieft: Zentral und heikel zugleich ist die Zuweisung der Rollen von Controller, Processor und Joint Controller. Während die Abgrenzung theoretisch klar scheint, stellen sich in der Praxis zahlreiche Fragen, die dringend zu klären sind. Derweil drängen alle in die Cloud, insbesondere in der Bankenszene wird derzeit stark dafür geworben. Doch inwieweit steht das mit dem Datenschutz und den Berufsgeheimnissen im Konflikt? Die Meinungen gehen hier diametral auseinander, und dies betrifft nicht nur die Banken, sondern etwa auch die Anwälte. Und wie lässt sich mit dem US-Cloud Act umgehen? Noch grundlegender herausgefordert wird der Datenschutz im Bereich der Distributed Ledger Technology (DLT). Wer kümmert sich um den Schutz von Personendaten in einer Datensammlung, deren Inhaber jeder und keiner ist? Und kann das Recht auf Löschung und Berichtigung durchgesetzt werden, wenn etwa eine Blockchain auf den ersten Blick darauf angelegt ist, dass Daten weder gelöscht noch korrigiert werden können? Diesen Fragen widmet sich das Schweizer Forum für Kommunikationsrecht (SF-FS) in der 3. Datenschutz-rechtstagung.

Programm

13:45 – 14:00
Einführung
Prof. Dr. FLORENT THOUVENIN, Tagungsleiter, Universität Zürich
DAVID ROSENTHAL, Tagungsleiter, Rechtskonsulent, Zürich

14:00 – 14:30
Update DSGVO: Die Urteile, die Bussen und was nun klar ist
Dr. DAVID VASELLA, Rechtsanwalt, Zürich

14:30 – 15:00
Update DSG: Neues aus der Fallpraxis des EDÖB
Dr. ADRIAN LOBSIGER, Eidgenössischer Datenschutzbeauftragter

15:00 – 15:30
Diskussion

15:30 – 16:00
Pause

16:00 – 16:30
Controller - Processor - Joint Controller: ein Rollenspiel
JULIETTE HOTZ, MLaw, Senior Counsel, Data Governance, Swisscom AG

16:30 – 17:00
Banken & Co. in die Cloud: Stehen der US-Cloud Act und das Berufsgeheimnis im Weg?
DAVID ROSENTHAL, Rechtskonsulent, Zürich

17:00 – 17:30
Datenschutz in der Blockchain: Sind neue Konzepte nötig?
KENTO REUTIMANN, MLaw, Zürich

17:30 – 18:00
Diskussion

ab 18:00
Apéro

# 3. DATENSCHUTZRECHTSTAGUNG

## Datenschutz in Bewegung

Update DSGVO: Die Urteile, die Bussen und was nun klar ist

Dr. DAVID VASELLA, Rechtsanwalt, Zürich

Update DSGVO:

# Urteile, Bussen und erste Klärungen

Schweizer Forum für Kommunikationsrecht
3. Datenschutzrechtstagung: Datenschutz in Bewegung

David Vasella
29. Mai 2019

walderwyss rechtsanwälte

## Leitlinien der Behörden

Auswahl

## EDPB, Entwurf Guidelines 3/2018 (räumlicher Anwendungsbereich)

- keine Anwendbarkeit nur aufgrund Auftragsverarbeitung im EWR
- keine Anwendbarkeit wegen Mitarbeitern im EWR
- Verhaltensbeobachtung:
  - Absicht, Daten in intensiver Weise einzusetzen (analog Profiling)
  - aber wohl auch Offline-Verhalten
- weiterhin viele Unklarheiten



## EDPB, Entwurf Guidelines 2/2019 (Verarbeitung für Verträge)

- keine Lösung: Datenbearbeitung als artifizieller Vertragsbestandteil
- restriktive Haltung, vertragsnahe Handlungen oft nicht gedeckt:
  - Empfehlungen gestützt auf Kundenverhalten
  - Betrugsprävention
  - Verbesserungen des Angebots
  - Werbepersonalisierung (auch nicht bei werbefinanzierten Angeboten!)

## DSK, Orientierungshilfe für Anbieter von Telemedien

- § 15 Abs. 3 TMG (Privilegierung des Online-Tracking bei Pseudonymisierung): nicht mehr anwendbar
- eher restriktive Auslegung des berechtigten Interesses
- Einwilligung: div. Hinweise zu Cookie Banner



# Rollenverteilung
## Controller, Processor, Joint Controller

## Controller und Processor

- Trend hin zu Controller/Controller oder Joint Controller-Verhältnissen
- Hilfestellungen der Behörden
  - BayLDA zur Abgrenzung Controller und Processor
  - LfDI BaWü: Muster für Joint Controller



## Joint Controller

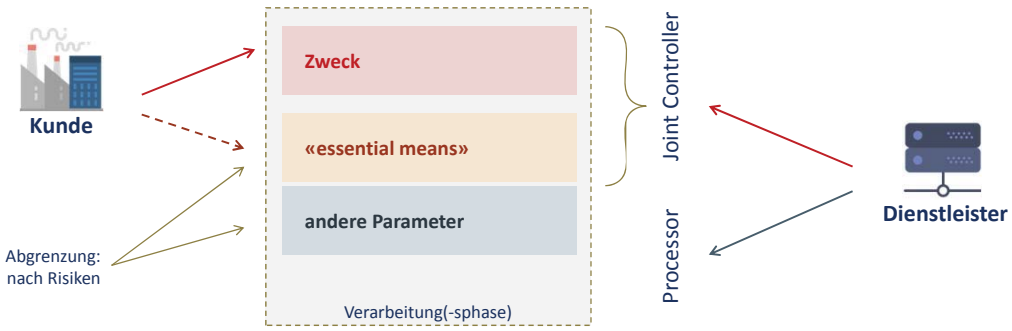
- **Wirtschaftsakademie Schleswig-Holstein**: (C-210/16, Urteil vom 5.6.18): Facebook-Fanpages
- **Zeugen Jehovas** (C-25/17, Urteil vom 10.07.18): Spendensammlung durch Mitglieder
- **Fashion ID** (C-40/17, Anträge des AG vom 19.12.18): Like-Buttons

## Joint Controller

- **kein Datenzugang** erforderlich
- **Kriterien:**
  - *Veranlassen* der Verarbeitung wesentlich, aber nicht ausreichend
  - *Zusatzelement*:
    - Organisieren/Koordinieren der Verarbeitung (Zeugen Jehovas)
    - Parametrierung der Verarbeitung (Facebook)
    - aktives Einbinden eines Like-Buttons (Fashion ID)
- gemeinsame V. auf **bestimmte Verarbeitungsphasen** beschränkt (z.B. Beschaffung und Weitergabe)



## Schema



## Sonstige laufende Diskussionen

walderwyss rechtsanwälte

## Anforderungen an Datenschutzerklärungen

- CNIL i.S. Google (Entscheid vom 21.1.2019):
  - heikel: mehrfache Verweisungen auf andere Dokumente (z.B. AGB)
  - heikel: vage Umschreibungen der Zwecke und Daten
  - Aufbewahrungsfrist: Angabe von Frist oder Kriterien (Motive der Aufbewahrung ungenügend)
  - hohe Anforderungen an Einwilligungen

- BVwG Österreich (Urteil vom 10.12.2018):
  - Zweckangaben: relativ konkret. Zu allgemein:
    - "Verbesserung der Benutzerfreundlichkeit"
    - "Marketingzwecke"
    - "Zwecke der IT-Sicherheit"
    - "künftige Forschung"
    - etc.
  - Faustregel: mind. 3 Worte pro Zweck

## Recht auf Kopie

- Recht auf Kopie ausdrücklich verankert – aber Umfang strittig
- BayLDA, TB 17/18: Recht auf Kopie der Daten, aber nicht von Dokumenten oder sonstigen Unterlagen
- LG Köln (Urteil vom 18.3.2019):
  - Auskunftsrecht und Recht auf Kopie: nicht betr. Dokumenten, sondern nur ggf. enthaltenen Personendaten
  - kein Auskunftsrecht betr. Personendaten, die der betroffenen Person (z.B. als Teil von E-Mails) bereits bekannt sind



## Kopplungsverbot

- gilt nicht absolut
- weniger streng bei unentgeltlichen Angeboten
  - OGH AT (Urteil vom 31.8.2018); kostenpflichtiges Angebot, TV: Vermutung des Verbots bei Kopplung
  - DSB AT (Beschluss vom 30. November 2018); kostenloses Angebot, Zeitung: Kopplungsverbot nur, falls beträchtliche negative Folgen oder Risiko einer Täuschung, Einschüchterung oder Nötigung

## One Stop Shop

- One Stop Shop (1SS) für Konzerne ohne HQ im EWR?
  - Leitbehörde = “main establishment” oder “single establishment” im EWR
  - Was gilt bei HQ ausserhalb des EWR, aber mehreren EWR-Niederlassungen?
  - CNIL i.S. Google: kein 1SS bei Google, da Entscheidung über die fraglichen Verarbeitungen nicht durch Google Ireland Ltd., sondern in den USA getroffen



# Enforcement

## Übersicht

- DPO: Registrierung von > 375’000 Unternehmen
- Breach Notification: > 89’000
- Beschwerden: > 144’000
- Bussen:
  - diverse Verfahren hängig; wenige veröffentlichte Entscheidungen
  - Faktoren bei der Bemessung (gemäss CNIL i.S. Google):
    - Bedeutung der verletzten Bestimmungen (Rechtmässigkeit und Transparenz sind Kernbestimmungen)
    - Dauerhaftigkeit und Umgang der verletzenden Verarbeitung; Anzahl betroffener Personen
    - Datenlastigkeit des Geschäftsmodells des Verantwortlichen
  - Kooperation wird belohnt (Knuddels)



## Strengere Praxis absehbar

**RGPD : « La Cnil sera plus ferme envers les entreprises » annonce sa présidente Marie-Laure Denis**

Par **Sylvain Rolland** | 15/04/2019, 15:34 | 2232 mots

Kurswechsel beim Datenschutz

**Vom Berater zum Kontrolleur**

Von Daniel Gräfe - 19. April 2019 - 16:24 Uhr

Landesdatenschützer Stefan Brink hat angekündigt, die Zahl der Kontrollen massiv zu erhöhen und die Beratung zurückzufahren. Was das für Firmen und Vereine bedeutet.

## Abmahnwesen




## Sicht der Unternehmen

## Anwendung der DSGVO

- häufig freiwillige Anwendung der DSGVO als Grundsatz…
- … mit Ausnahmen, z.B.
  - bei den Betroffenenrechten, besonders der Mitarbeiter
  - bei Geoblocking und Werbesperren
  - bei Einzelfallentscheidungen
- … und generell mehr Mut, die DSGVO nicht anzuwenden
  - Beruhigung des Themas
  - weniger Angst vor Behörden
  - Vollstreckung in der Schweiz unwahrscheinlich



## Datenschutzverletzungen

- Datenschutzverletzungen werden erkannt (?) und i.d.R. rasch bearbeitet
- meist Bagatellfälle (z.B. Fehlversand von E-Mails)
- Meldungen:
  - als Ausnahme
  - im Staat des EU-Vertreters
  - bei Niederlassungen im EWR: ggf. kein 1SS!

## Umsetzungsarbeiten

- Stand:
  - Umsetzungsarbeiten dauern an
  - viele Projekte am Anfang, erste Projekte aber abgeschlossen (…)
  - erste DSG-Projekte laufen
- Erkenntnis: Prozesse statt Dokumente!
- bestimmte Einzelfragen werden vertiefter geprüft
  - Controller vs Processor
  - Information von indirekt betroffenen Personen
  - Vertragsgestaltung
  - Umfang der Betroffenenrechte



# Bilanz nach dem 1. Jahr

## Unternehmenssicht

- gewisse Beruhigung
- als Thema intern etabliert
- Aufbau interner Ressourcen
- gestiegener Aufwand bei Verträgen



## Das grössere Ganze

- DSGVO hat Vorbildfunktion:
  - "common frame of reference"
  - Inspiration für ausländische Gesetze
- … aber wirklich Stärkung des Datenschutzes? Alternative Sichtweisen möglich:
  - DSGVO zur Abwehr anderer Regulierungen (z.B. Kartellrecht)
  - DSGVO zur Perpetuierung der Autonomiefiktion
  - DSGVO als verkapptes Technologiesteuerrecht
  - **G**enerating **D**isproportionate **P**artner **R**eturns?

# Vielen Dank.

RA Dr. David Vasella, CIPP/E
david.vasella@walderwyss.com
+41 58 658 52 87

walderwyss rechtsanwälte

# 3. DATENSCHUTZRECHTSTAGUNG

## Datenschutz in Bewegung

Update DSG: Neues aus der Fallpraxis des EDÖB

Dr. ADRIAN LOBSIGER, Eidgenössischer Datenschutzbeauftragter

# Aus der Fallpraxis des EDÖB

## zu Privatsphäre und Informationeller Selbstbestimmung

Sophie Haag

Adrian Lobsiger

Schweizer Forum für Kommunikationsrecht, Uni Zürich, 29. Mai 2019

Bundesdatenschutz zuständig für die

# Bearbeitung von Personendaten

## Durch private Personen

- 600'000 Schweizer Firmen (12'000 mittlere und grosse)
- 130'000 Vereine und Stiftungen
- 8 Millionen Benützer von digitalen Applikationen

Bundesdatenschutz zuständig für die

# Bearbeitung von Personendaten

## Durch Private Personen

600'000 Schweizer Firmen (12'000 mittlere und grosse)
130'000 Vereine und Stiftungen
8 Millionen Benützer von digitalen Applikationen

## Durch Bundesorgane

Bundesverwaltung, bundesnahe Betriebe, Hochschulen etc.

## Fallpraxis EDÖB

Fallpraxis EDÖB

# 1. Helsana+ Urteil des BVerG vom 19.3.2019

2. Aufsichtsverfahren des EDÖB i. S. ZEK
3. Massenauskunftsgesuche via App
4. Datenbeschaffungen im Vorfeld von Abstimmungen

Fallpraxis EDÖB

# 1. Helsana+ Urteil des BVerG vom 19.3.2019

"Mit dem Urteil des BVerG ist nun hoffentlich klar, dass das Datenschutzrecht kein Vehikel ist, andersartigen Regelungszielen zum Durchbruch zu verhelfen."

Daniel Vasella, 29.3.2019

Fallpraxis EDÖB 

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Faktische Rückerstattung von Grundversicherungsprämien als Entgeld von Datenlieferung**

Fallpraxis EDÖB 

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Kombination von**

- Digitale Applikation – personalisierte Datenbearbeitung
- Konzerngesellschaften
- AGBs

Faktische Rückerstattung von Grundversicherungsprämien als Entgeld von Datenlieferung – **Umgehung / Rechtsmissbrauch**

Fallpraxis EDÖB 

1. Helsana+ Urteil des BVerG vom 19.3.2019

Rechtsbegehren

Rechtswidrige Datenbearbeitung sei zu unterlassen und rechtwidrig bearbeitete Daten zu löschen.

Fallpraxis EDÖB 

1. Helsana+ Urteil des BVerG vom 19.3.2019

Nicht: Moral, Ethik, Konsumentenschutz oder übergesetzliche Gerechtigkeit oder Wahrheit

Keine Urteilsschelte

Fallpraxis EDÖB

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Deal:** Daten der Grundversicherten gegen CHF 75.- der Zusatzversicherung

- **Keine** Unzulässige Koppelung
- Begründet **nicht** Unfreiwilligkeit der Einwilligung

Fallpraxis EDÖB

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Rechtswidrigkeit**

- **Keine** Benachteiligung (CHF 75.--)
- **Keine** missbräuchliche Berufung auf rechtliche Trennung der Gesellschaften
- **Keine** Finanzmittel der Grundversicherung

Fallpraxis EDÖB

1. Helsana+ Urteil des BVerG vom 19.3.2019

Deal: Daten der Grundversicherten gegen CHF 75.- der Zusatzversicherung

Ist die Datenlieferung und die App nötig zur Erbringung der gesetzlichen Grundsversicherungsleistung ?

Ist Preisgabe der Daten wirklich freiwillig, bei Rabatt von X %?

Fallpraxis EDÖB

1. Helsana+ Urteil des BVerG vom 19.3.2019

Art 84a KVG

Keine Norm, die direkt oder indirekt, den Schutz der Persönlichkeit einer Person bezweckt

Fallpraxis EDÖB

Lehre: Begründung der Rechtswidrigkeit nicht auf derartige Normen fokussieren

1. Helsana+ Urteil des B[illegible]vom 19.3.2019

Art 84a KVG

Keine Norm, die direkt oder indirekt, den Schutz der Persönlichkeit einer Person bezweckt

Fallpraxis EDÖB

1. Helsana+ Urteil des BVerG vom 19.3.2019

3. Varianten

- DSG an DSGVO anpassen
- DSG unverändert lassen
- Explizite Regelung der personalisierten Prämienrabatte im KVG (Motion Humbel)

Fallpraxis EDÖB

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Datentransfer Grundversicherung zu Zusatzversicherung**

- **Nicht** schrankenlos (Umfang und Zweck)
- **AGB** sind anzupassen unabhängig von der tatsächlichen Praxis

Fallpraxis EDÖB

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Art 84a KVG**

- Einwilligung im **Einzelfall**
- Unterschrift
- Einwilligung gegenüber Bundesorganen als Surrogat für gesetzliche Grundlage (Vasella)

Fallpraxis EDÖB

## 1. Helsana+ Urteil des BVerG vom 19.3.2019

**Fazit:**

- Bald altrechtlicher Fall
- Ev. erfolgen gesetzgeberische Schritte
- Koppelungsverbot und Freiwilligkeitsargument haben Potential
- Einschränkung der Normenkognition beschränkt Aufsicht EDÖB

Fallpraxis EDÖB

## 2. Aufsichtsverfahren des EDÖB i S ZEK

- Weiterentwicklung der Praxis Moneyhouse
  - Prüfquote Interessennachweise
  - Prüfquote Datenrichtigkeit

Fallpraxis EDÖB

## 2. Aufsichtsverfahren des EDÖB i S ZEK

- Prüfquote *Interessenachweise*
  - Missbrauchsrisiko ausschlaggebend
    - Zugang zur Datenbank nur für Mitglieder
    - Mitglieder werden auditiert

  → wesentlich tiefere Prüfquote akzeptiert

Fallpraxis EDÖB

## 2. Aufsichtsverfahren des EDÖB i S ZEK

- Prüfquote *Datenrichtigkeit*
  - Prüfmöglichkeiten der Betroffenen mitberücksichtigt
    - Betroffene werden über Datenbearbeitung informiert
  - ursprüngliche Datenqualität

  → wesentlich tiefere Prüfquote akzeptiert

Fallpraxis EDÖB

## 3. Massenauskunftsgesuche via App

- Sind solche (durch Dritte) gestellten Gesuche gültig?
- Wie können diese gesetzeskonform und mit vernünftigem Aufwand bearbeitet warden?

Fallpraxis EDÖB

## 3. Massenauskunftsgesuche via App

- Grundsätzlich gültiges Auskunftsgesuch, aber...

Legitimation auskunftsersuchende Person muss geprüft werden

Fallpraxis EDÖB

## 3. Massenauskunftsgesuche via App

- gesetzeskonformer Umgang mit Massengesuchen
  - automatisierte Antwort mit Aufforderung zur Spezifizierung und Legitimation
  - Ev. Link auf Firmenwebsite mit Webformular und Upload-Möglichkeit

Fallpraxis EDÖB

## 4. Datenbeschaffungen im Vorfeld von Abstimmungen

- Sympathisanten geben politischen Akteuren Daten Dritter bekannt, die für Stimmempfehlungen und Reminder verwendet werden

→ Daten können unter das erhöhte Schutzniveau besonders schützenswerter Personendaten fallen

Fallpraxis EDÖB

## 4. Datenbeschaffungen im Vorfeld von Abstimmungen

- Information
- Jederzeit widerrufbare Einwilligung

Fallpraxis EDÖB

## 4. Datenbeschaffungen im Vorfeld von Abstimmungen

Zum Ganzen: Leitfaden Wahlen und Abstimmungen, erstellt durch die Datenschutzbehörden von Bund (EDÖB) und Kantonen (Privatim)

www.derbeauftragte.ch → Datenschutz → Leidfäden → Wahlen und Abstimmungen

# 3. DATENSCHUTZRECHTSTAGUNG

## Datenschutz in Bewegung

Controller - Processor - Joint Controller: ein Rollenspiel

JULIETTE HOTZ, MLaw, Senior Counsel, Data Governance, Swisscom AG


## Rollen bei der Verarbeitung personenbezogener Daten

**Hauptakteure**

| Betroffene Person | Controller | Processor | Sub-Processor |
|---|---|---|---|
| • Gibt Daten selbst bekannt<br>• Daten werden über ihn gesammelt | • Verantwortet die Datenverarbeitung<br>• Ansprechstelle für betroffene Person | • Verarbeitet Daten gemäss Weisung des Controllers | • Verarbeitet Daten (via Processor) gemäss Weisung des Controllers |

Vertrag (zwischen Controller und Processor)

Vertrag (zwischen Processor und Sub-Processor)

| Dritter | Empfänger | Unter der Aufsicht eines Controllers oder Processors |
|---|---|---|
| • Anderer als Hauptakteure und in deren unmittelbaren Verantwortung Stehende | • Person […] der Daten offen gelegt werden<br>• Unabhängig von rechtlicher Qualifikation | • Processor und<br>• Controller oder Processor unterstellte (einzel-) Person, die Zugang zu Daten hat<br>• Unmittelbare gesetzliche Pflicht zur Verarbeitung gemäss Weisung des Controllers<br>• (Kein ADV mit Freelancern etc.) |

## Processor



### Kriterien

- Verarbeitet personenbezogene Daten ausschliesslich zum vom Controller vorgegebenen Zweck
- Untersteht einem Weisungsrecht, das sich spezifisch auf die Datenverarbeitung bezieht

### Hinweis, jedoch nicht ausreichend

- Datenverarbeitung zum mittelbaren Zweck der Vertragserfüllung gegenüber einem Kunden
- Datenverarbeitung zu keinem eigenen Zweck
- Daten vom Kunden erhalten, bzw. von diesem zugänglich gemacht
- Auftragsrechtliches Weisungsrecht des Kunden
- Schuldrechtliche Herausgabepflicht bezüglich der Daten

### Beispiele

- IT-Outsourcing
- Auslagerung HR-Dienstleistungen

### Auswirkung

- Privilegierung Datenweitergabe
- Rechtfertigung der Datenverarbeitung



## Sole Controller



### Kriterien

- Entscheidet alleine über Mittel und Zweck der Verarbeitung personenbezogener Daten

### Zweck

- Ob und wozu Daten (an sich) verarbeitet werden
- Nicht zu verwechseln mit Ziel eines Auftrags zwecks dessen Erfüllung Daten verarbeitet werden

### Mittel

- Wesentliche Mittel
  Insb. welche Daten, welche Quellen, wo verarbeitet, wie ausgewertet, mit welchen verknüpft, wie lange gespeichert, von wem verarbeitet
- Entscheid über restliche Mittel, insb. TOMs führen in der Regel nicht zu Verantwortlichkeit

### Beispiele

- Entwicklungstätigkeit eines IT-Unternehmens
- Führung einer Datenbank mit Geschäftskontakten

### Auswirkung

- Trägt Verantwortung für Einhaltung DSGVO
- Trägt Bussenrisiko, bei Verletzung

## Joint Controller

**Kriterien**

- Veranlasst (in gewissem Mass) Verarbeitung personenbezogener Daten und
- Entscheidet mit über Mittel oder Zweck der Verarbeitung personenbezogener Daten
- Nicht erforderlich: Zugang zu den Daten
- Nicht erforderlich: Wille des Dienstleisters Verantwortlicher zu sein
- Nicht erforderlich: Ausdrückliches Verlangen der Datenverarbeitung

**Beispiele**

- Facebook Fanpages: Einfluss auf Parametrierung der verarbeiteten Daten
- Zeugen Jehovas: Schaffung des Umfelds und der Organisation, Möglichkeit Verarbeitung zu verhindern

**Auswirkung**

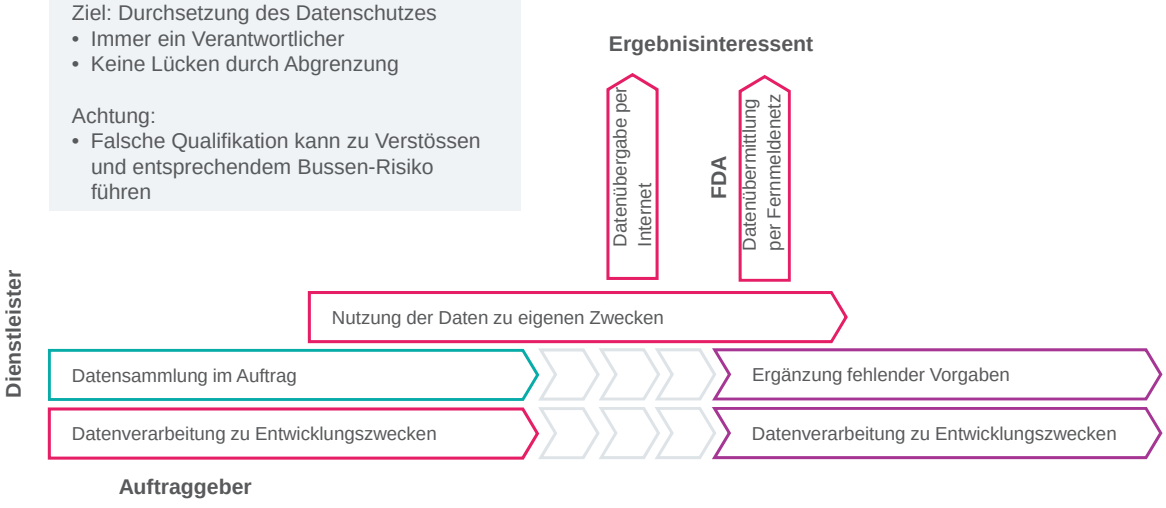
- Trägt Verantwortung für Einhaltung DSGVO
- Trägt Bussenrisiko, bei Verletzung, solidarische Haftung aller Controller



## Rollenspiel

Ziel: Durchsetzung des Datenschutzes
- Immer ein Verantwortlicher
- Keine Lücken durch Abgrenzung

Achtung:
- Falsche Qualifikation kann zu Verstössen und entsprechendem Bussen-Risiko führen



## Regelung der Verhältnisse und Rollengestaltung

| | | |
|---|---|---|
| **Controller** | ADV Art. 28<br>Weisungsrecht<br>Unterstützungspflicht | **Processor** |
| **Joint Controller** | Vertrag Art. 26<br>Verteilung<br>Verantwortlichkeiten | **Joint Controller** |
| **Controller** | Keine Vorschrift<br>Empfehlenswert | **Controller** |

Die Rollen und Ausprägungen sind mit Bedacht zu gestalten. Sie haben alle ihre Vor- und Nachteile. Frei wählen lässt sich die Rolle allerdings nicht.
Fallback:
Wer muss aus Sicht der betroffenen Person für die Datenverarbeitung verantwortlich sein?



**Kontakt**

Swisscom (Schweiz) AG
Data Governance
Juliette Hotz
Pfingstweidstrasse 51
8004 Zürich

juliette.hotz@swisscom.com

# 3. DATENSCHUTZRECHTSTAGUNG

## Datenschutz in Bewegung

Banken & Co. in die Cloud: Stehen der US-Cloud Act und das Berufsgeheimnis im Weg?

DAVID ROSENTHAL, Rechtskonsulent, Zürich

Homburger

# Banken & Co. in die Cloud

Stehen der US CLOUD Act und das Bankgeheimnis im Weg?

**David Rosenthal**
29. Mai 2019

Version 1.01

Homburger

## Alle wollen in die Cloud ...

- **Wir tun es** mit unseren privaten Computern, Tablets, und Handies
  - iCloud, GMail, OneDrive, Office365, etc.
  - Viele Apps und Programme erfordern es inzwischen
- **Viele Betriebe** tun es oder wollen es
  - Ersparnisse, Flexibilität, Innovation, Datensicherheit
- Für einmal schlagen die **Versicherungen** die Banken
  - Helsana entschied sich 2015 als erster Krankenversicherer, mit Kundendaten in die Cloud zu gehen – und tat es unter Einbezug der FINMA und des BAG
  - Etliche Versicherer speichern ihre Daten im Ausland oder in der Cloud oder bereiten dies vor
- Zwei Branchen tun sich jedoch noch schwer, jedenfalls was Kundendaten betrifft
  - Schweizer **Banken**
  - Schweizer **Anwälte**

Hans-Peter Keller, CIO, Helsana
"Wir waren die Ersten, die mit dem CRM in die Cloud gingen"

Homburger

## Was steht dem entgegen?

- **FINMA Outsourcing Rundschreiben** und andere aufsichtsrechtliche Vorgaben
  - On-site Audit-Rechte ✓
  - Beizug von Unterbeauftragten ✓
  - Möglichkeit des Exit und der Rückführung ✓
  - Garantierter Datenzugriff ✓
  - ~~Pflicht zur Kundeninformation in AGB|Schreiben~~ ✓
- **Datenschutz** ✓
  - DSGVO ist strenger als das Schweizer Recht
  - Vertragliche Regelung ist unproblematisch
- **Datensicherheit** ✓
  - Mit den entsprechenden Cloud-Angeboten besser als beim Eigenbetrieb
- **Berufsgeheimnis ?**
  - Art. 47 BankG (Banken)
  - Art. 321 StGB (Anwälte, Ärzte, etc.)
- **US CLOUD Act ?**
  - Angst vor jederzeitigem Zugriff auf Daten durch die US-Regierung
- **Meinung der Kunden und Öffentlichkeit, wenn Schweizer Banken in die internationale Cloud gehen ?**
  - Negativschlagzeilen?
  - Verlust von Kundenvertrauen?



Homburger

## Berufsgeheimnis

- **Geheimnisträger**
  - Anwalt, Hilfsperson, Bankangestellter, Beauftragter
- **Materielles Geheimnis**
  - Relativ unbekannte Tatsache, an welcher der Kunde ein Geheimhaltungsinteresse hat und die dem Geheimnisträger in seiner beruflichen Funktion anvertraut wurde oder die er wahrgenommen hat
- **Tatbestand ist die Offenbarung an unbefugte Dritte**
  - Zur Kenntnis bringen, Kenntnisnahme ermöglichen
  - Kenntnisnahme durch den Dritten erforderlich
  - Aus der Vereinbarung mit dem Kunden ergibt sich, wer unbefugt ist und wer nicht
- **Vorsätzliche und tw. fahrlässige Verletzung bestraft**

**Art. 321**

1. Geistliche, Rechtsanwälte, Verteidiger, Notare, Patentanwälte, nach Obligationenrecht[368] zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Chiropraktoren, Apotheker, Hebammen, Psychologen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.[369]

StGB

**Art. 47**[157]

[1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird bestraft, wer vorsätzlich:

a.[158] ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Organ, Angestellter, Beauftragter oder Liquidator einer Bank oder einer Person nach Artikel 1*b* oder als Organ oder Angestellter einer Prüfgesellschaft anvertraut worden ist oder das er in dieser Eigenschaft wahrgenommen hat;

b. zu einer solchen Verletzung des Berufsgeheimnisses zu verleiten sucht;

c.[159] ein ihm nach Buchstabe a offenbartes Geheimnis weiteren Personen offenbart oder für sich oder einen anderen ausnützt.

[1bis] Mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe wird bestraft, wer sich oder einem anderen durch eine Handlung nach Absatz 1 Buchstabe a oder c einen Vermögensvorteil verschafft.[160]

[2] Wer fahrlässig handelt, wird mit Busse bis zu 250 000 Franken bestraft.

BankG

## Das eigentliche Problem ...

- Nicht: **Kenntnisnahme durch den Cloud-Anbieter** selbst
  - Auslagerungen an einen IT-Service-Provider grundsätzlich zulässig (kein unbefugter Dritter)
    - Sofern sie die üblichen Voraussetzungen erfüllen (Datensicherheit)
    - Herrschende Lehre (u.A. SCHWARZENEGGER|THOUVENIN|STILLER, a.M.WOHLERS) und Praxis
  - Gelten als Hilfspersonen bzw. Beauftragte (schliesst sie dies als unbefugte Dritte aus?)
    - Unterstehen in der Schweiz ebenfalls dem Berufsgeheimnis
- Nicht: **Unrechtmässiger Zugriff durch Dritte** (z.B. Hacker, interne Datendiebe)
  - Verlangt wird nur aber immerhin, dass eine angemessene Datensicherheit betrieben wird
- Sondern: **Rechtmässiger Zugriff durch ausländische Gerichte|Behörden** ("lawful access")
  - Ausländischer Provider untersteht lokalem Recht, welches ihn zur Offenlegung zwingt
  - Wurde diese Offenbarung an einen Dritten fahrlässig oder eventual-vorsätzlich ermöglicht?
  - Wenn nichts im Vertrag steht: Hat ein vernünftiger Kunde dieses Risiko akzeptiert oder nicht?





## Die Charmeoffensive der Bankenbranche

- **Lösungsansatz:** Bank trifft die vernünftigerweise von ihr zu erwartenden Massnahmen zum Schutz der Daten vor Behördenzugriffen → kein Vorsatz|keine Fahrlässigkeit
- **Technische Massnahmen** (z.B. Verschlüsselung von Daten, ohne dass der Provider den Schlüssel kennt = BYOK) lösten das Problem nicht, da sie je nach Modell bisher mit zu erheblichen Einschränkungen verbunden waren oder die Möglichkeit einer "Hintertür" bestand
- **Organisatorische Massnahmen** (z.B. Möglichkeit zur Anfechtung von Zugriffsbegehren) sind im Ausland an sich kein geeignetes Mittel gegen ausländisches Recht
- **Fazit: Keine befriedigende Antwort** auf das Problem
  - Welches Restrisiko muss ein Kunde akzeptieren?
  - Auch die Kundeninformation wird ausgeblendet


die Möglichkeiten der Bank und ihres Kunden, sich gegen einen Zugriff mit rechtlichen Mitteln zur Wehr zu setzen (weil das Risiko eines Zugriffs im Rahmen eines rechtsstaatlichen Verfahrens auch bei in der Schweiz liegenden Daten besteht und die Auslagerung ins Ausland nicht per se untersagt ist und bei einer entsprechenden Anfrage auch Rechtfertigungsgründe vorstellbar sind, genügt die Bank ihren diesbezüglichen Sorgfaltspflichten typischerweise dann, wenn sichergestellt wird, dass sie bzw. der betroffene Bankkunde eine entsprechende Anfrage in einem rechtsstaatlichen Verfahren überprüfen lassen können);

Gutachten WalderWyss, S. 27

**Offenlegung von Kundendaten**

Microsoft legt keine Kundendaten außerhalb von Microsoft oder ihren kontrollierten Tochtergesellschaften und verbundenen Unternehmen offen, außer es geschieht (1) auf Anweisung des Kunden, (2) wie in den OST beschrieben oder (3) wie gesetzlich vorgeschrieben.

Microsoft wird Kundendaten nicht gegenüber Strafverfolgungsbehörden offenlegen, sofern nicht gesetzlich vorgeschrieben. Sollte sich eine Vollstreckungsbehörde mit Microsoft in Verbindung setzen und Kundendaten anfordern, versucht Microsoft, die Vollstreckungsbehörde an den Kunden zu verweisen, damit sie diese Daten direkt beim Kunden anfordert. Wenn Microsoft verpflichtet ist, Kundendaten gegenüber einer Vollstreckungsbehörde offenzulegen, wird Microsoft den Kunden unverzüglich darüber informieren und ihm eine Kopie der Aufforderung zukommen lassen, sofern dies nicht gesetzlich verboten ist.

Microsoft Bestimmungen für Onlinedienste ("OST") vom 1. Mai 2019





## US CLOUD Act – zu Recht ein Schreckgespenst?

- Klarstellung im "**Stored Communications Act**" (SCA)
- Gewisse Kategorien von US-IT-Providern (inkl. Cloud Provider) **müssen Kundendaten offenlegen**, die in ihrem physischen **Besitz** oder unter ihrer **Kontrolle** sind
  - Nur für Strafuntersuchungen
  - Erfordert einen Gerichtsbeschluss
  - Neu wird klargestellt, was an sich schon bisher galt: Es spielt keine Rolle, *wo* sich die Daten befinden
- Diese Regelung entspricht der Cybercrime Convention (Art. 18), welche seit 2012 auch für die Schweiz gilt
  - Die Schweiz hat sie freizügiger umgesetzt: Zugriffe auf die Cloud erfolgen i.d.R. ohne Gerichtsbeschluss
- **Fazit:** Nichts Neues, nichts Dramatisches
- Teil 2 des CLOUD Act schafft die Möglichkeit von sog. **Executive Agreements** mit anderen Staaten
  - Regeln, in welchen Fällen Zugriffe erlaubt sind, *ohne* das betroffene fremde Recht zu berücksichtigen
  - UK handelt eines aus, EU erwägt ebenfalls eins, aber es gibt erhebliche Bedenken betr. Datenschutz
  - Soll als Alternative zur Rechtshilfe diese entlasten
- Wenn kein Executive Agreement besteht: US-Gericht muss das Prinzip der "international comity" beachten und die US und ausländischen **Interessen abwägen**, wenn der Zugriff ausländisches Recht verletzen würde
  - Datenschutzrecht, Bankgeheimnis, Art. 271 StGB
- **Fazit:** Ein Executive Agreement ist wohl keine Lösung

Homburger

## Wann sind Daten "unter der Kontrolle" des Providers?

- Papier des **US-Justizministeriums** vom April 2019
  - Verweist ebenfalls auf die Cybercrime-Konvention und dessen erläuternden Bericht des Europarats
- Provider muss demnach die Möglichkeit haben, die Erfüllung des Herausgabebefehl **aus den USA heraus ohne relevante Einschränkung steuern** zu können
  - Eine reine technische Zugriffsmöglichkeit genügt nicht unbedingt; relevant ist auch, ob die Kontrolle legitim ist
- US-Gerichte wendeten in anderen Fällen bisher **zwei Tests an**
  - Kann der Provider im Rahmen seines normalen Geschäftsbetriebs die Daten verlangen und darauf zuzugreifen ("practical ability test")? Es sind diverse Faktoren zu berücksichtigen
  - Hat der Provider ein Recht, mit dem er die Daten herausverlangen kann ("legal right test")
- **Fazit:** Vom Provider wird nicht verlangt, dass er seine Systeme hackt oder eine Hintertür einbaut

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Auszug aus dem Explanatory Report
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185



Homburger

## Wie können wir damit umgehen?

- **Option 1:** Das Risiko eines "lawful access" einer ausländischen Behörde wird stillschweigend akzeptiert
  - Für die meisten Branchen akzeptabel
  - Auch inländische Daten unterliegen der Rechts- und Amtshilfe und die meisten Behörden fragen direkt an
- **Option 2:** Kunden informieren bzw. einwilligen lassen
  - Kunden tragen das Risiko des Zugriffs
  - Wer Angst hat, seine Kunden zu fragen, geht selbst davon aus, dass auch Option 1 keine Lösung ist
- **Option 3:** Daten in EU-Cloud, weitgehende Abschottung
  - BYOK, zwar keine durchgängige Verschlüsselung, aber Zugriff auf Daten wäre nur durch Hacking oder Hintertür möglich; Vertrag sagt, dass es keine gibt
- **Option 4:** Daten nur dauerverschlüsselt in der Cloud
  - BYOK mit durchgängiger Verschlüsselung bis in den Chip (z.B. Microsofts "Confidential Compute" → löst viele Nutzungseinschränkungen, aber nicht alle)
- **Option 5:** US-Provider, aber Daten in der Schweiz
  - z.B. O365 auf Microsofts Schweizer Data Center
  - Mit oder ohne Wartungszugriff aus dem Ausland; in letzterem Fall ggf. kundengesteuert (z.B. Lockbox)
  - Zugriff auf Daten zwecks Herausgabe an US-Behörden wäre weltweit nach Art. 271 StGB strafbar
- **Option 6:** Reine Schweizer Cloud
  - SIX Swiss Cloud und andere CH-Hosting-Anbieter

Homburger

## Fazit

- **Schweizer Banken** sind aufgrund des Bankgeheimnisses in einer Sonderposition
  - **Erwartungshaltung** des typischen Bankkunden, die sich aber im Laufe der Zeit ändern wird
  - In anderen Branchen sollte anderen Risiken (z.B. *Business Continuity*) mehr Augenmerk beigemessen werden, da sie grösser sind als ausländische Behördenzugriffe
- Es ist **nur eine Frage der Zeit**, bis Banken & Co. mit ihren Kundenaten in die Cloud gehen
  - Schon heute nur noch eine wesentliche Hürde: Die Gefahr eines rechtmässigen **Zugriffs durch ausländische Behörden** auf Kundendaten im Klartext
  - Hierfür entwickeln sich derzeit praktikable **Lösungsansätze**; die praktische Umsetzung und die Nachweise der Sicherheit wird nicht ganz einfach sein
- Die Diskussion dominieren allerdings vor allem **diffuse Ängste**
  - Angst **vor dem US CLOUD Act** – zu Unrecht ein Schreckgespenst, da er einen viel engeren und weniger weitgehenden Anwendungsbereich hat, als die meisten befürchten
  - Angst **vor dem Kunden** – dass er negativ reagiert, wenn ein Unternehmen in die Cloud geht



Homburger

## Vielen Dank für Ihre Aufmerksamkeit!

lic. iur. David Rosenthal
david.rosenthal@homburger.ch
T +41 43 222 16 69

# 3. DATENSCHUTZRECHTSTAGUNG

## Datenschutz in Bewegung

Datenschutz in der Blockchain: Sind neue Konzepte nötig?

KENTO REUTIMANN, MLaw, Zürich

WEINMANN ZIMMERLI

Marken- & Patentanwälte
Rechtsanwälte
Trademark & Patent Attorneys
Attorneys at Law

# Datenschutz in der Blockchain: Sind neue Konzepte nötig?

SF·FS – Schweizer Forum für Kommunikationsrecht

3. Datenschutzrechtstagung – Datenschutz in Bewegung

Kento Reutimann

29. Mai 2019

## Ausgangslage

### Geschichte

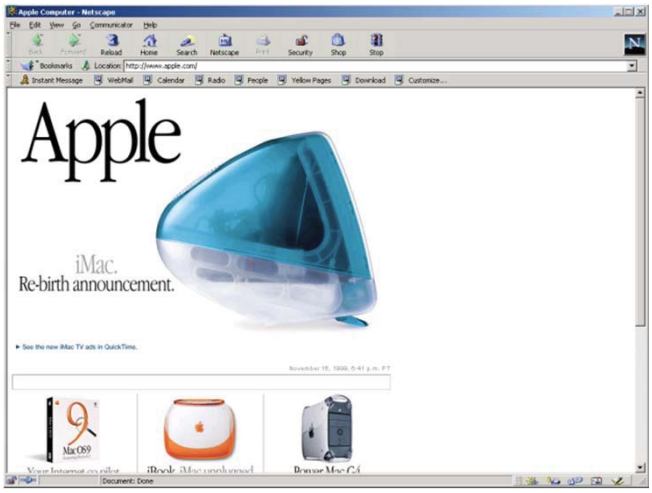
**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

## Ausgangslage

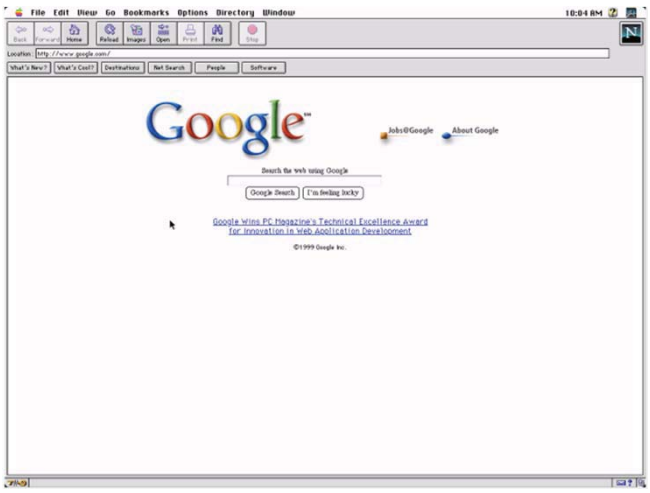
### Geschichte






## Ausgangslage

### Geschichte



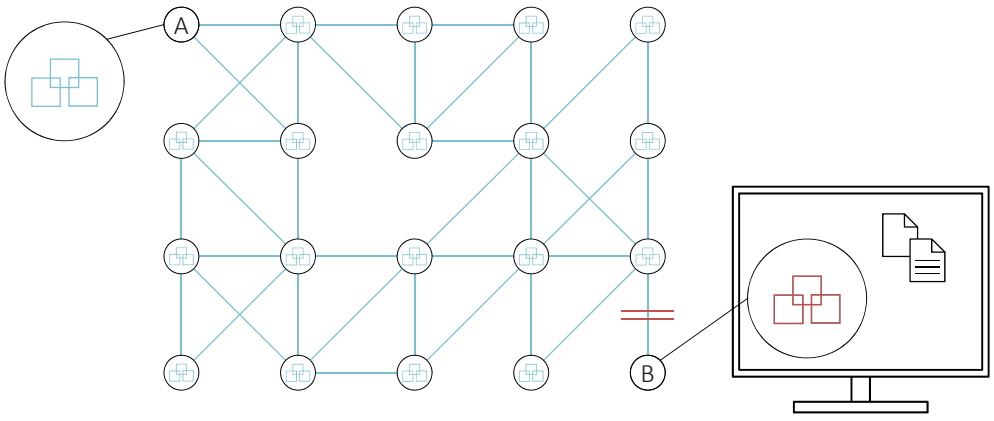
## Ausgangslage

### Technologie



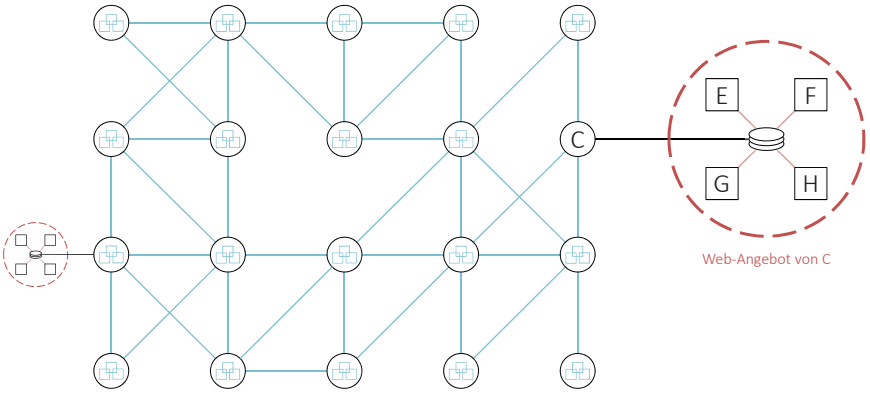

## Ausgangslage

### Technologie



## Ausgangslage

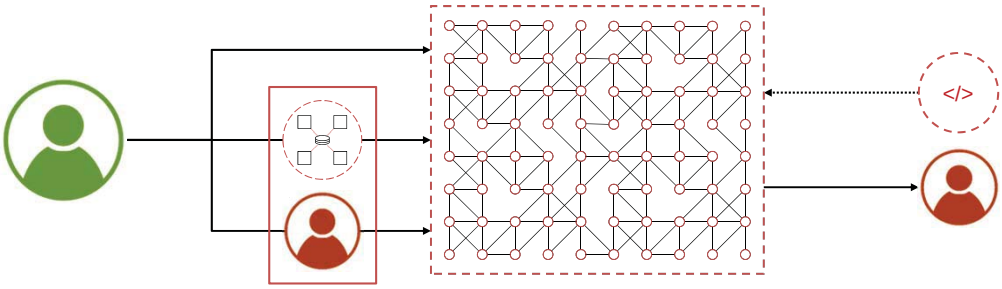
### Technologie






## Ausgangslage

### Akteure



## Ausgangslage

### Objekt der datenschutzrechtlichen Analyse

| | Permissionless | Permissioned |
|---|---|---|
| **Public** |   ethereum |  E O S™ |
| **Private** |  LTO Network |  HYPERLEDGER FABRIC |



## Ausgangslage

### Objekt der datenschutzrechtlichen Analyse

- Blockchain als System?
- einzelne Transaktion?
- Smart Contract/DApp/DAO?

## Datenschutzrecht

- Recht auf informationelle Selbstbestimmung
- DSGVO: Entwicklung in Richtung Konsumentenschutz
- DSG und DSGVO gehen von einer zentralen Instanz aus, welche die Kontrolle ausübt
  → Dezentralität ist nicht vorgesehen
- Territorialität



## Anwendungsbereich

- Bearbeiten
  - jeder Umgang mit Personendaten
  - insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten
- Personendaten
  - Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen
  - relativer Beurteilungsmassstab (EuGH vom 19. Oktober 2016, C-582/14 – Breyer)
  - Singularisierung ausreichend

## Normadressaten

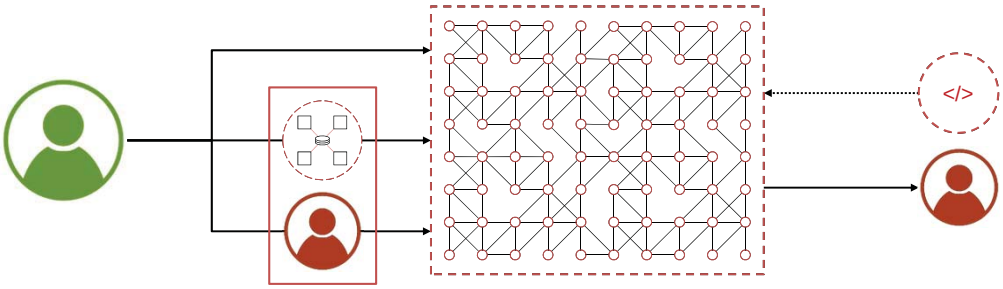
| DSG | E-DSG | DSGVO |
|---|---|---|
| **Inhaber einer Datensammlung** (Art. 3 lit. i)<br>"private Personen oder Bundesorgane, die **über den Zweck und den Inhalt der Datensammlung entscheiden**" | **Verantwortlicher** (Art. 4 lit. i)<br>"private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen **über den Zweck und die Mittel der Bearbeitung entscheidet**" | **Verantwortlicher** (Art. 4 Abs. 7)<br>"die natürliche oder juristische Person […], die allein oder gemeinsam mit anderen **über die Zwecke und Mittel der Verarbeitung** […] **entscheidet**" |
| **Bearbeiter**<br>Person, welche Personendaten bearbeitet | **Auftragsbearbeiter** (Art. 4 lit. j)<br>"private Person oder Bundesorgan, die oder das **im Auftrag des Verantwortlichen Personendaten bearbeitet**" | **Auftragsverarbeiter** (Art. 4 Abs. 8)<br>"eine natürliche oder juristische Person […], die personenbezogene Daten **im Auftrag des Verantwortlichen verarbeitet**" |
| **Dritter**<br>Person, welche kein Bearbeiter ist | **Dritter**<br>? | **Dritter** (Art. 4 Abs. 10)<br>"eine natürliche oder juristische Person […], **außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter** […]" |



## Normadressaten: Verantwortlicher (DSGVO)

- Weiter Begriff
  - Wirtschaftsakademie Schleswig-Holstein, EuGH vom 5. Juni 2018, C-210/16
- Gemeinsame Verantwortlichkeit: keine Voraussetzung, dass jeder Akteur Zugang zu den personenbezogenen Daten hat
  - Jehovan todistajat, EuGH vom 10. Juli 2018, C-25/17, Rn. 69

## Normadressaten im Blockchain-Kontext






## Gemeinsam Verantwortlicher: Verantwortlich für was?

- Wirtschaftsakademie Schleswig-Holstein (EuGH vom 5. Juni 2018, C-210/16)
  - "Klarzustellen ist, dass das Bestehen einer gemeinsamen Verantwortlichkeit (...) aber nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat (...). Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmass in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller massgeblichen Umstände des Einzelfalls zu beurteilen ist." (Rn. 43)

## Gemeinsam Verantwortlicher: Verantwortlich für was?

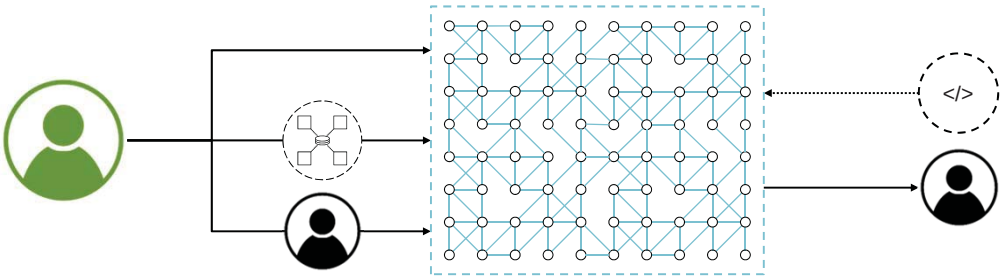
- Ausgangspunkt: "für die Verarbeitung Verantwortlicher"
  - Verarbeitung: zielt auf einen konkreten Vorgang oder eine Vorgangsreihe ab
  - Verantwortlich: Entscheidung über Zweck und Mittel
  - Fashion ID (Schlussanträge des GA vom 19. Dezember 2018, C-40/17)
    - Beschränkung der Verantwortlichkeit eines gemeinsam Verantwortlichen auf diejenigen Verarbeitungsvorgänge, für die er tatsächlich einen Beitrag zur Entscheidung über die Mittel und Zwecke der Verarbeitung leistet (Rn. 108)



## Grundsätze der Datenbearbeitung

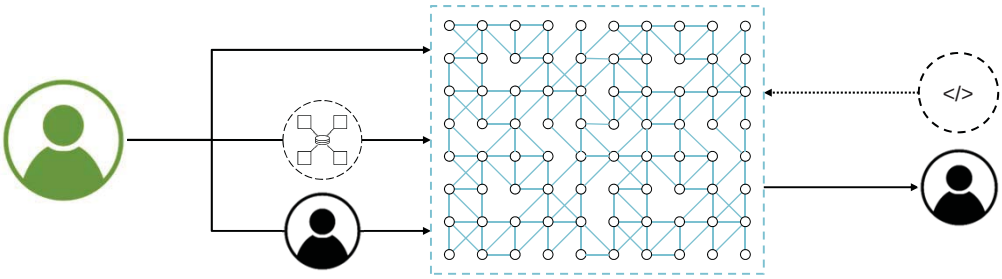
| DSG | DSGVO |
|---|---|
| Rechtmässigkeit (Art. 4 Abs. 1) | Rechtmässigkeit (Art. 5 Abs. 1 lit. a) |
| Bearbeitung nach Treu und Glauben (Art. 4 Abs. 2) | Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a) |
| Verhältnismässigkeit (Art. 4 Abs. 2) | Datenminimierung (Art. 5 Abs. 1 lit. c)<br>Speicherbegrenzung (Art. 5 Abs. 1 lit. e) |
| Erkennbarkeit (Art. 4 Abs. 4) | Transparenz (Art. 5 Abs. 1 lit. a) |
| Zweckbindung (Art. 4 Abs. 3) | Zweckbindung (Art. 5 Abs. 1 lit. b) |
| Richtigkeit der Daten (Art. 5) | Richtigkeit der Daten (Art. 5 Abs. 1 lit. d) |
| Datensicherheit (Art. 7) | Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) |

## Rechtfertigung durch Einwilligung






## Rechtfertigung durch überwiegende Interessen



## Recht auf Berichtigung

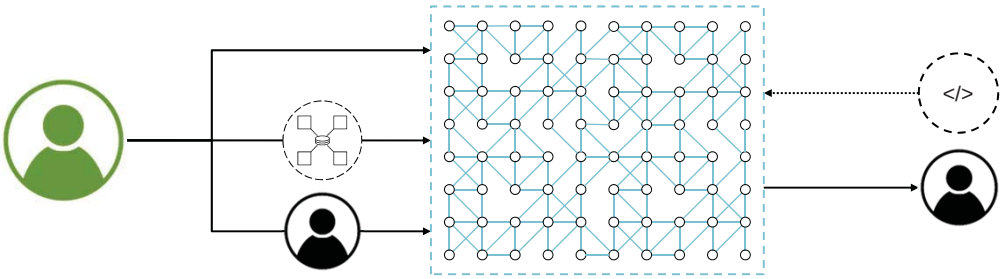
- Schweiz: Art. 15 Abs. 1 i.V.m. Art. 5 Abs. 2 DSG
  - Anspruch erfordert eine widerrechtliche Verletzung der Persönlichkeit
  - Widerrechtlichkeit liegt nicht vor, wenn ein Rechtfertigungsgrund vorliegt (s.a. Art. 28 Abs. 2 ZGB)
- EU: Art. 16 DSGVO
  - Anspruch richtet sich gegen Verantwortlichen
  - Möglichkeit einer ergänzenden Erklärung ausreichend
  - Teil der Lehre fordert Interessenabwägung



## Recht auf Löschung

- Schweiz: Art. 15 Abs. 1 DSG
  - Anspruch erfordert eine widerrechtliche Verletzung der Persönlichkeit
  - Widerrechtlichkeit liegt nicht vor, wenn ein Rechtfertigungsgrund vorliegt (s.a. Art. 28 Abs. 2 ZGB)
- EU: Art. 17 DSGVO
  - Anspruch richtet sich gegen den Verantwortlichen
  - Voraussetzungen (Abs. 1), z.B.
    - Widerspruch der betroffenen Person, sofern keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen
    - Unrechtmässige Verarbeitung

## Datenschutzrechtliche Beurteilung






## Datenschutzfördernder Einsatz der Blockchain-Technologie

- Förderung des Datenschutzes auf Blockchains
  - Personendaten nicht direkt auf Blockchains speichern, sondern nur referenzieren
  - Zero-Knowledge-Proofs (zk-SNARKs, zk-STARKs)
  - Einsatz von zusätzlichen Ebenen (z.B. Enigma)
  - Sidechains
- Förderung des Datenschutzes durch Blockchains
  - E-Identity
  - Personal Information Management Systems / Personal Data Vaults




WEINMANN ZIMMERLI

Marken- & Patentanwälte
Rechtsanwälte
Trademark & Patent Attorneys
Attorneys at Law

Kento Reutimann
MLaw

Apollostrasse 2, 8032 Zürich
k.reutimann@weinmann-zimmerli.ch
www.weinmann-zimmerli.ch