

Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# Dateneigentum und Datenzugang: Herausforderungen in der Praxis

**29. November 2017, 14:00 – 18:00 Uhr**  
**Universität Zürich**  
**Rämistrasse 59, 8001 Zürich**  
**Raum RAA-G-01**

Mit der Digitalisierung haben Daten für Staat und Wirtschaft massiv an Bedeutung gewonnen. Schon heute sind Daten für immer mehr Unternehmen das wichtigste Asset, zumindest bei der Entwicklung künftiger Geschäftsmodelle. Dies wirft die grundlegende Frage auf, wem alle diese Daten gehören. Das geltende Recht kann dazu nur partielle Antworten geben. Dies wirft die in Theorie und Praxis derzeit intensiv diskutierte Frage auf, ob ein allgemeines „Dateneigentum“ geschaffen werden sollte.

Das Center for Information Technology, Society, and Law (ITSL) der Universität Zürich hat diese Frage im Rahmen eines Forschungsprojekts untersucht und ist zum vorläufigen Schluss gekommen, dass die Einführung eines allgemeinen „Dateneigentums“ nach heutigem Kenntnisstand kaum sinnvoll wäre. Damit ist die Sache freilich nicht erledigt. Denn zum einen wirft die faktische Herrschaft von Unternehmen über riesige Datenbestände die Frage auf, ob in gewissen Konstellationen spezifische Zugangsrechte zu Daten erforderlich sind. Zum anderen bestehen verschiedene praktische Probleme, die allenfalls mit einem allgemeinen „Dateneigentum“ gelöst werden könnten und die nun andere Lösungen erfordern.

Das Schweizer Forum für Kommunikationsrecht (SF-FS) und das ITSL untersuchen diese Fragen im Rahmen einer Veranstaltung. Nach einer Bestandsaufnahme stehen die praktischen Fragen im Vordergrund: Wie sind Daten im Konkurs oder im Erbgang zu behandeln? Inwieweit ist „Web Scraping“ zulässig? Und welche Möglichkeiten bestehen, wenn Datenträger abhandengekommen und die Daten auf diesen gelöscht und anderswo gespeichert worden sind?

## Programm

Leitung: Prof. Dr. ROLF H. WEBER und Prof. Dr. FLORENT THOUVENIN,  
beide Universität Zürich

### Grundsatzfragen

14:00 – 14:30 Zum Bedarf nach einem Dateneigentum  
Prof. Dr. ROLF H. WEBER und Prof. Dr. FLORENT THOUVENIN

14:30 – 14:45 Schutz von Geschäftsgeheimnissen als Alternative?  
Prof. Dr. PETER GEORG PICHT, Universität Zürich

14:45 – 15:00 Zum Bedarf nach Datenzugangsrechten  
Dr. ALFRED FRÜH, Universität Zürich

### Herausforderungen in der Praxis

15:00 – 15:20 Web Scraping  
Dr. DEMIAN STAUBER, Rechtsanwalt, Zürich

15:20 – 15:40 Personal Information Management Systems (PIMS)  
CLARA-ANN GORDON, Rechtsanwältin, Zürich

15:40 – 16:10 Kaffeepause

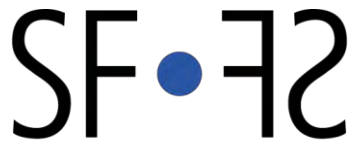
16:10 – 16:35 Verlust von Daten  
Dr. GREGOR BÜHLER, Rechtsanwalt, Zürich

16:35 – 16:55 Daten im Konkurs  
Dr. PETER K. NEUENSCHWANDER, Rechtsanwalt, Zollikon

16:55 – 17:15 Daten im Erbgang  
LENNART CHROBAK, Universität Zürich

17:15 – 18:00 **Plenumsdiskussion**  
Moderation: Prof. Dr. FLORENT THOUVENIN

ab 18:00 Apéro



Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Zum Bedarf nach einem Dateneigentum**

**Prof. Dr. ROLF H. WEBER und Prof. Dr. FLORENT THOUVENIN**





# Zum Bedarf nach einem Dateneigentum

Prof. Dr. Rolf H. Weber / Prof. Dr. Florent Thouvenin

Universität Zürich / Rechtswissenschaftliches Institut  
Center for Information Technology Society and Law – ITSL

Zürich, 29. November 2017



## Ausgangslage bei Sach- und Personendaten

**Sachenrecht**

**Immaterialgüterrecht**

Urheberrecht

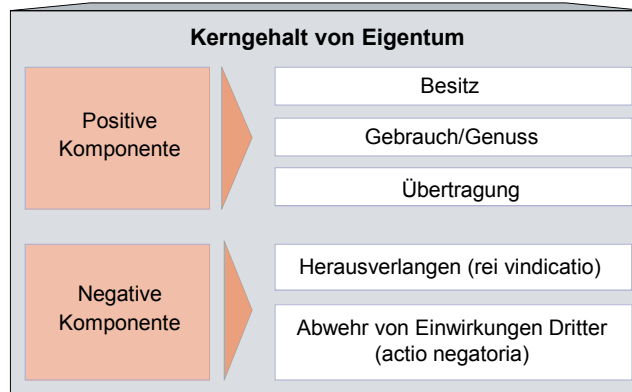
Nachbarrechte

Datenbankenschutz (sui generis)

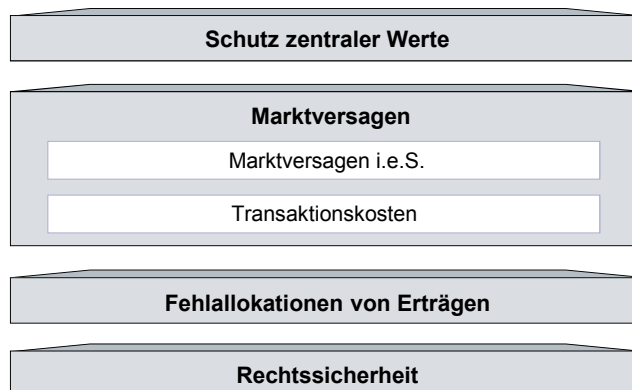
**Wettbewerbsrecht (UWG)**

**Deliktsrecht**

### Ausgangslage bei Personendaten



### Rechtfertigung eines Dateneigentums



## Herausforderungen bei der Einführung von Dateneigentum

Probleme  
bei der  
Ausgestaltung

Probleme  
bei der  
Implementierung

Mögliche  
Folgeprobleme

## Ausgestaltung: Gegenstand und Zuordnung

### Gegenstand des Rechts

Daten als unbestimmter Begriff

Bedeutung der Ebene der Daten

### Zuordnung der Daten

Berechtigung der die Daten betreffenden Person

Berechtigung der die Daten verarbeitenden Person / Institution

Formen des Miteigentums



### Ausgestaltung: Rahmenbedingungen

Umschreibung der vermittelten Rechte

Übertragbarkeit des Eigentums

Zeitliche Begrenzung des Eigentums?

Publizität des Eigentums



### Verwendung von Distributed Ledgers

Eigentum ohne Publizität

Rechtsqualität der Datenpakete

Kontrolle der Infrastruktur

Gewähr der Rechtssicherheit





### Implementierung: Verhältnis zum Datenschutzrecht

#### Parallelität von Dateneigentum und Datenschutzrecht

Widersprüche

Pattsituationen

#### Verdrängung des Datenschutzrechts durch Dateneigentum

Erhaltenswerter Kern des Datenschutzrechts

Zugangsverweigerung zu eigenen Daten



### Mögliche Folgeprobleme

Schwierige  
Rechtsfolgeabschätzung

Erhöhtes  
Monopolisierungsrisiko

Notwendigkeit der  
Einführung neuer  
Rechtsinstrumente



## Zusammenfassende Erkenntnisse

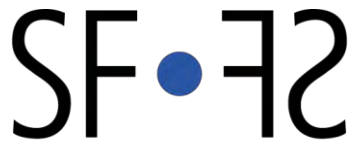
### Fehlendes Marktversagen

Wirtschaftliche Aspekte

Zentrale Werte

### Spezifisch zu behebende Regelungslücken

Vermeidung des Eintritts unerwünschter  
faktischer oder rechtlicher Folgen



Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Schutz von Geschäftsgeheimnissen als Alternative?**

Prof. Dr. PETER GEORG PICTH





# Dateneigentum und Datenzugang – Schutz von Geschäftsgeheimnissen als Alternative?

Prof. Dr. Peter Georg Picht, LL.M. (Yale)



## Heutiger Rechtsrahmen des Schutzes von Geschäftsgeheimnissen

- **Begriffliches: «Know-How» & «Geschäftsgeheimnis»**
  
- **Rechtliche Rahmenbedingungen**
  - Art. 39 TRIPS (*Schutz vertraulicher Informationen*)
  - Art. 2, Art. 4 lit. c und Art. 6 UWG (*Fabrikations- und Geschäftsgeheimnisse*)
  - Art. 5 UWG (*Verwertung fremder Leistungen*)
  - Art. 162 StGB (*Verletzung des Fabrikations- und Geschäftsgeheimnisses*)
  - Art. 321a OR (*Treuepflicht des Arbeitnehmers*)
  - Weitere Normen
  
- **Ökonomische Relevanz ⇔ fehlende «Verdinglichung» zum Immaterialgüterrecht**



## Ordnungsrahmen für die Datenwirtschaft? – Modellszenario „Connected Mobility“

- Vielfältige und umfangreiche **Datenerzeugung**
- Schwierige Abgrenzung **Personendaten** ↔ **Sachdaten**
- Vielzahl beteiligter **Akteure** (Fahrer, Halter, Hersteller, Infrastrukturanbieter, Aggregator, Serviceprovider...)
- Überlagerung verschiedener **Rechtsbereiche** (Vertragsrecht, Lauterkeitsrecht, Immaterialgüterrecht, ...)
- Erhebliche **Gestaltungsmacht** einzelner «Vertragssetzer»



[http://www.bmi.vde/SharedDocs/DE/Publikationen/DG/eigenumsordnung-mobilitaetdaten.pdf?\\_\\_blob=publicationFile](http://www.bmi.vde/SharedDocs/DE/Publikationen/DG/eigenumsordnung-mobilitaetdaten.pdf?__blob=publicationFile)



## Ordnungsrahmen für die Datenwirtschaft? – Einige offene Fragen

- Grundsätzliche Schutzzfähigkeit digitaler Daten als «Geschäftsgeheimnisse»
- Schutzebene: Semantisch oder syntaktisch?
- Identifikation des „richtigen“ Schutzbegünstigten durch Geheimhaltungskriterium?
- Schutz unternehmensbezogener Geschäftsgeheimnisse ausreichend?



## Ordnungsrahmen für die Datenwirtschaft? – Einige offene Fragen

- Klärung insbes. des Verhältnisses zum Datenschutzrecht und Immaterialgüterrecht
  
- Erwünschte Enforcement-Struktur?
  
- Geheimnischarakter als Schutzvoraussetzung ⇔ zugangsorientierte Datenwirtschaft
  - Beeinträchtigung dynamischer Effizienz
  - Datenmacht – Informationsfreiheit – Wettbewerb
  - Neukonzeptionierung der «Geheimhaltung» erforderlich & iRd Geschäftsgeheimnisschutzes möglich?



## Entwicklungen in der EU und Schweiz

- **EU-Richtlinie 2016/943/EU über den Schutz vertraulichen Know-Hows und vertraulicher Geschäftsinformationen**
  - Schon unklar, ob/wann Daten überhaupt erfasst
  - Geheimhaltungsanforderungen: Verringerung des bisherigen Schutzzumfangs? Zugangsorientierung?
  - Anwendungsvorbehalt zugunsten sonstiger relevanter Vorschriften → Kein eigenständiges Abstimmungskonzept zwischen den Rechtsbereichen
  - Keine grundlegende Neuorientierung an Bedürfnissen der Datenwirtschaft



## Entwicklungen in der EU und Schweiz

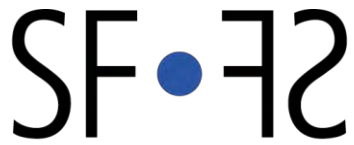
- **EU Strategie für einen digitalen Binnenmarkt:**
  - Unjustified data location restrictions: Wohl Fokus auf Speicherort
  - Proposal for a Regulation on a framework for the free flow of non-personal data: Vertragsbasierte Selbstregulierung als Grundansatz
  
- **Strategie «Digitale Schweiz»:** (Bisher) keine Bezugnahme auf Know-How-Schutz



## Fazit

- Gewisse **grundlegende Eignungszweifel**
- Jedenfalls weitreichender **Klärungs- und Anpassungsbedarf**, sofern Umbau des Geschäftsgeheimnisschutzes zu einem Ordnungsrahmen für die Datenwirtschaft angestrebt
- Sofern **andere(r) Ordnungsrahmen** bevorzugt:
  - Koexistenz als **partieller Lösungsansatz** möglich
  - **Abstimmungsbedarf**, damit Geschäftsgeheimnisschutz nicht zum **Störfaktor** wird





Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Zum Bedarf nach Datenzugangsrechten**

Dr. ALFRED FRÜH





# Zum Bedarf nach Datenzugangsrechten

SF-FS | ITSL

Dateneigentum und Datenzugang: Herausforderungen in der Praxis  
29. November 2017

*Alfred Früh*

## 1) Ausgangspunkt

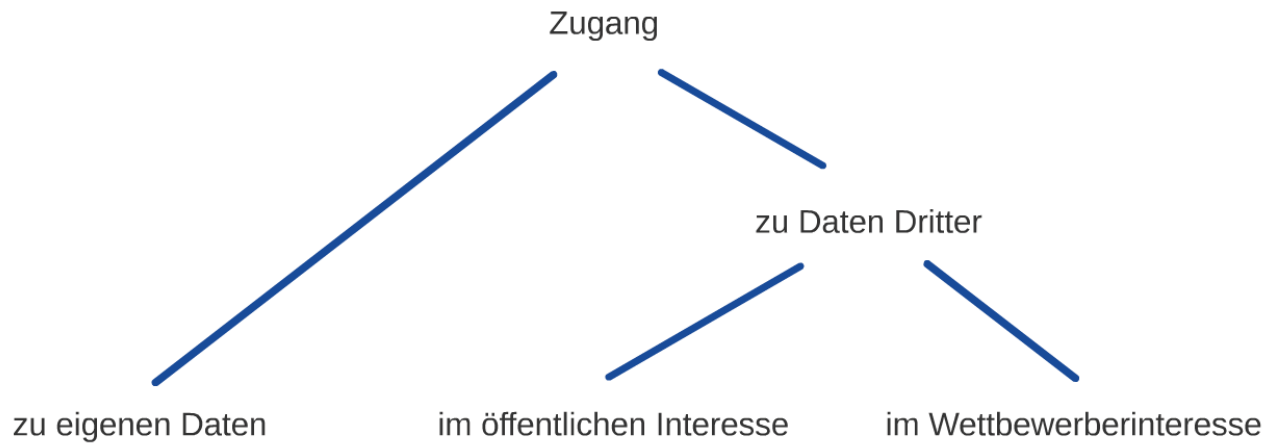
### Rechtliche Zuordnung von Daten

- Teilweise Zuordnung durch bestehende Instrumente
- Neue, übergreifende Regelung unerwünscht
- Punktuell besteht Handlungsbedarf

### Faktische Zuordnung von Daten

- Datenbestände sind faktisch gegen Zugriff geschützt
- Punktuell bestehen Zugangsrechte
- ➡ • Bedürfnis nach (einem) übergreifenden Zugangsrecht(en)?

## 2) Systematisierung möglicher Datenzugangsrechte



## 3) Zugang zu eigenen Daten

- Wiedererlangung faktischer Kontrolle über Daten
  - Speicherung bei Dritten ohne vertragliche Vereinbarung
  - Verlust eines Datenträgers
  - Verlust des Zugriffs über nicht besonders gesicherte Datenbestände
- Insbesondere wenn keine anderen Ansprüche bestehen
  - Datenschutzrecht: Auskunftsrecht gem. Art. 8 DSGVO, aber eben nur für Personendaten
  - Vertragsrecht: Entweder gar kein Vertrag oder Zugang vertraglich gültig abbedungen
  - Deliktsrecht: Widerrechtlichkeit und Verschulden können fehlen

Warum?

- Dem Besitzesrecht nachgebildetes neues Zugangsrecht
  - Rasche Wiederherstellung der tatsächlichen Herrschaft an Daten
  - Mit einfachen Mitteln durchsetzbar



Wie?

#### 4) Zugang zu Daten Dritter im öffentlichen Interesse

- Kontrolle von Daten in proprietären Silos kann Nutzung im öffentlichen Interesse verhindern
  - Google Trends: Pandemieprognosen aufgrund von Suchanfragen
  - Orange D4D: Verbreitung von Bilharziose mit anonymisierten Telefondaten
  - Nutzung von Randdaten bei der Strafverfolgung
- Von Privaten in der "hoheitlichen Sphäre" erhobene Daten sollten der Allgemeinheit zugutekommen ("Reverse PSI")
  - Daten über die Nutzung von Verkehrs- und Netzinfrastruktur
- Daten liefern bessere Entscheidungsgrundlagen für Behörden
  - Gesundheitswesen: Daten von Spitälern und Versicherungen
  - Gefahrenanalyse: Daten zu Hochwasser und Naturgefahren
  - Umweltschutz: Daten bezgl. Emissionen
  - Raumplanung: Daten zu Verkehrsinfrastruktur
  - Wirtschaftsförderung: Unternehmensdaten



Warum?

- Grundsätzliches
  - Übergreifende oder punktuelle Lösung
  - Konkrete Umsetzung des Zugangsrechts/der Zwangslizenz
  - Kenntnis von der Existenz der Daten
- Konkretes
  - Eingriffsvoraussetzungen
    - Berücksichtigung der Interessenlagen (insbes. Geschäftsgeheimnisse)
  - Lizenzgegenstand
    - Daten (syntaktisch, semantisch oder pragmatisch verstanden?)
    - Rohdaten oder veredelte Daten
  - Weiterverwendung
  - Lizenzgebühr

Wie?

## 5) Zugang zu Daten von Wettbewerbern

- Zugang zu Daten als unerlässliche Voraussetzung für die Tätigkeit auf einem Markt (insbes. vor- oder nachgelagerte Märkte)
  - Mehrstufige Liefer- und Leistungsketten wie in der Automobilindustrie
- Kartellrechtliches Eingreifen nicht zielführend
  - Verfahrensdauer
  - Mangelhafter Umgang des Kartellrechts mit Datenmärkten

Warum?

- Grundsätzliches
  - Übergreifende oder punktuelle Lösung?
    - Zugang zu Reparatur- und Wartungsinformationen (VO 715/2007)
    - Zahlungsinformation: Zugang für Fintech-Unternehmen (RL 2015/2366)
  - Konkrete Umsetzung des Zugangsrechts/der Zwangslizenz
- Konkretes
  - Eingriffsvoraussetzungen
    - Berücksichtigung der Interessenlagen (insbes. Geschäftsgeheimnisse)
  - Lizenzgegenstand
    - Daten (syntaktisch, semantisch oder pragmatisch verstanden?)
    - Rohdaten oder verddelte Daten
    - Anonymisierte Daten oder Personendaten
  - Weiterverwendung
  - Lizenzgebühr



Wie?

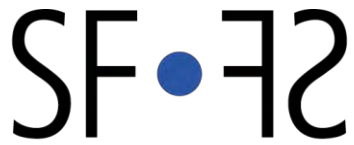
## 6) Rekapitulation / Ausblick

- Untersuchung der *faktischen* anstatt *rechtlichen* Zuordnung von Daten
- Zugangsrechte in mindestens drei Konstellationen
  - Mit jeweils unterschiedlichen Rechtfertigungen...
  - ...und Eingriffsvoraussetzungen
- Gemeinsamkeiten
  - Erfassung des Gegenstandes (Welche Daten? Welche Art von Daten?)
  - (Sektor-)spezifisch oder übergreifend

Vielen Dank für die Aufmerksamkeit.

*[alfred.frueh@rwi.uzh.ch](mailto:alfred.frueh@rwi.uzh.ch)*





Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Web Scraping**

Dr. DEMIAN STAUBER



# Web Scraping

Demian Stauber | Zurich, 29.11.2017

## Einleitung

- Web Scraping (aka screen scraping, Web harvesting oder Web data extraction)
  - (teil)-automatisiertes Extrahieren von (spezifischen) Daten aus Websites (und strukturierte Wiedergabe bzw. Weiterverwendung)
  - diverse Methoden und Anwendungsbeispiele
  
- Abgrenzung zu: Web Crawling – «Indexierung» nicht Extraktion von spezifischen Daten

## Einfach

ready-to-use Software...

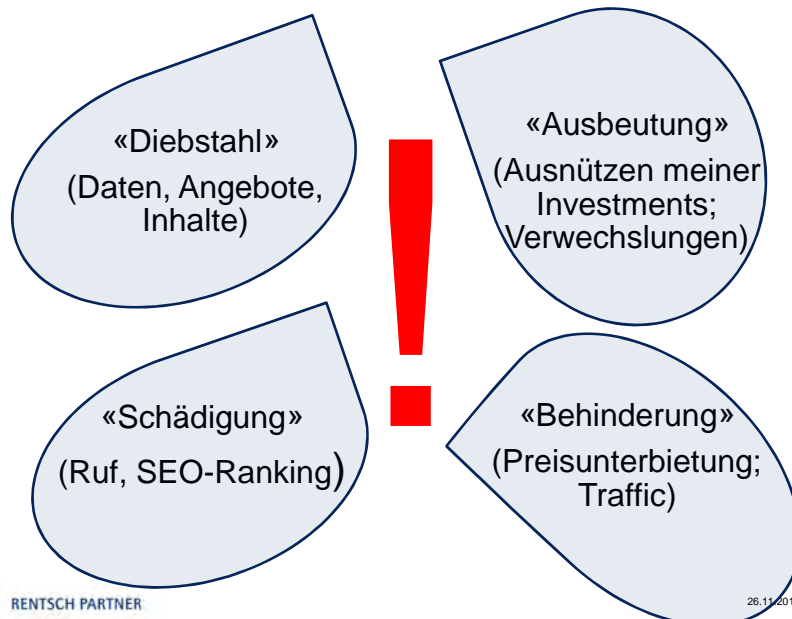
## Fortgeschritten

mit ein bisschen Programmieraufwand...

## Anwendungsbeispiele

- Auslesen von
  - Preisen (Flugpreise, Online-Katalogpreise etc.)
  - Adressen
  - Inseraten (Immobilien etc.)
  - anderen Daten (Wetter, Temperaturen, Sportergebnissen etc.)

## Vorwürfe

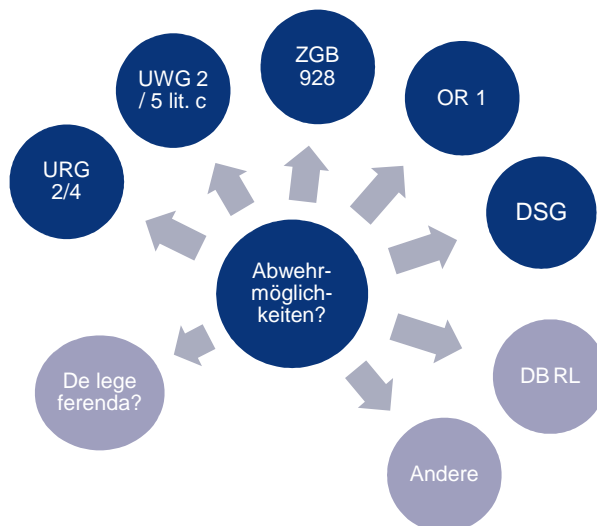


## Technische Abwehrmassnahmen

- Captcha
- Account erforderlich für Content-Abfrage (mit E-Mail-Adresse und Verifizierung o.ä.)
- IP Adressen blocken
- regelmässige HTML-Änderungen / Honeypot
- robots.txt (robots exclusion protocol)
- spezifische Software-Lösungen (z.B. in Firewall) inkl. «bad bot fingerprints, browsers validation, behavioral modeling etc.)

Leichter gesagt als getan: leichte Umgehung wenn nicht relativ hoher Aufwand, Beeinträchtigung erwünschter User

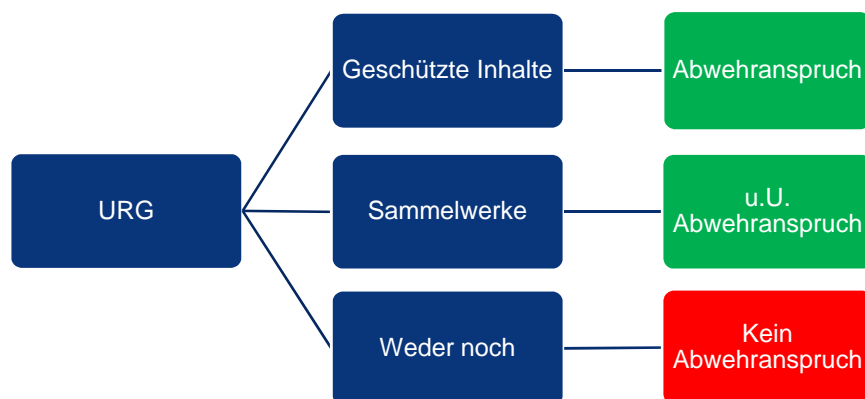
## Rechtliche Themen



## URG

| URG 2      |  |  |
|------------|--|--|
| Werk       | «Individualität»                               | i.d.R. nicht erfüllt bei Daten   |
|            | «Individualität»                               | Ausnahmen z.B.:<br>– Texte, die als Sprachwerke qualifizieren<br>– Bilder<br>– ggf. Fotografien            |
| URG 4      |  |  |
| Sammelwerk | «Individualität» bezügl. Auswahl und Anordnung | i.d.R. nicht erfüllt bei «logischen» Datenbanken («Arzneimittelkompendium – BGE 134 III 166»)              |
|            | «Individualität» bezügl. Auswahl und Anordnung | Ausnahmen z.B.:<br>– Rezepte- oder Witzesammlung<br>– Übernahme als Ganzes oder mind. «individuellem Teil» |

## URG



## UWG

| UWG 5 lit. c   |  |  |
|--|--|--|
| Fremdes marktreifes Arbeitsergebnis                        | Selbständig verwertbares «Produkt» inkl. Teile davon   | I.d.R. erfüllt (BGE 134 III 166 – Arzneimittelkompendium)  |
|  | <-> nicht selbständig verwertbare Teile  | Selektive Daten, z.b.<br>- Orte bei Immobilieninseraten<br>- «Theoriefragen» Autoprüfung (HGP Bern, sic 2016, S. 56) |
| Übernahme und Verwertung als solches / techn. Reproduktion | Unmittelbare Verwertung  | Diskutabel, wenn Daten sortiert, aufbereitet und in neuer Form zur Verfügung gestellt werden                         |
| Ohne angemessenen Eigenaufwand                             | Aufwand für die Reproduktion, allfällige Weiterentwicklung und Variation vs «Erstellungsaufwand» | Scraping mit Scraping-»Standard-Software« unzulässig, aber mit eigener Lösung schon?                                 |
| Amortisation   | BGE 131 III 384 / 134 III 166  | Taugliches Merkmal?  |

Aber: BGE 131 III 384 – Such-Spider (2005) – wirklich ein aktueller «leading case»? (Sachverhalt unvollständig – Eigenaufwand Klägerin nicht substantiiert / Eigenaufwand damals – heute <-> «Spidering» Kantonsgericht Freiburg vom 22. August 2016, sic! 2017, 228-236

11

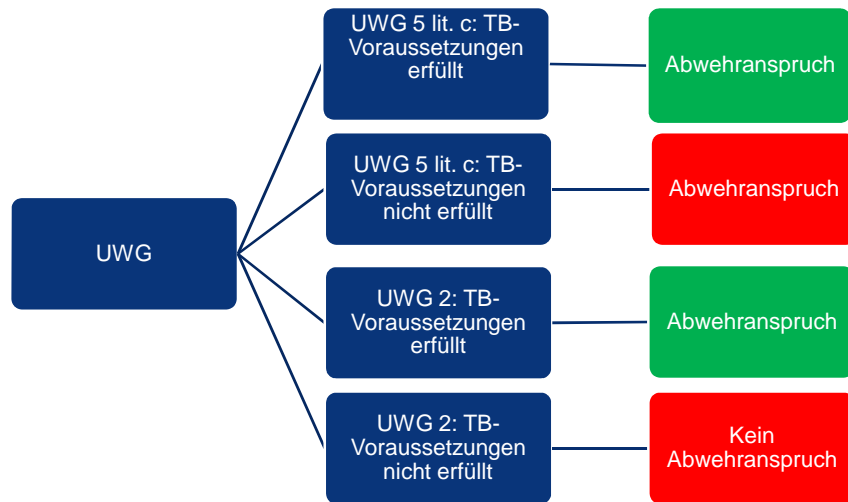
## UWG

| UWG 2            |  |  |
|------------------|--|--|
| Treu und Glauben | Fallgruppe «Ausbeuten fremder Leistung»    | Grds. nicht  |
|                  | Bei Umgehung technischer Schutzmassnahmen? | «Aufwand -> kein UWG 5 lit. c»<br>«besondere Umstände für Unlauterkeit?» |

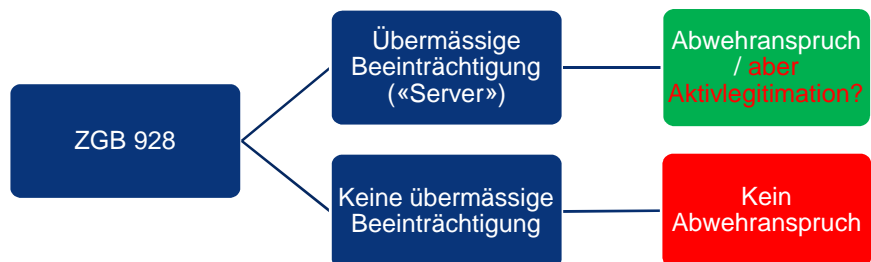
**Aber:** BGE 131 III 384, 308 – Such-Spider: «Das Internet enthält eine Vielzahl von Daten. Sind diese als solche nicht immaterialgüterrechtlich geschützt, sondern frei zugänglich, so erscheint es grundsätzlich sinnvoll, dass sich der Wettbewerb unter den Plattform-Betreibern über die an bestimmten Bedürfnissen des Publikums orientierte Vollständigkeit, Verlässlichkeit und Erschliessung dieser Daten abspielt.»



## UWG



## ZGB – Besitzstörung



## OR 1 - Vertragsschluss - Nutzungsbedingungen

### Nutzungsbedingungen / Haftungsausschlusserklärung

Mit dem Zugriff auf diese Webseite („UBS-Webseite“) anerkennen Sie die rechtlich bindende Wirkung der hier genannten Nutzungsbedingungen und des Haftungsausschlusses („Nutzungsbedingungen“). Bitte lesen Sie ausserdem die für Ihr jeweiliges Land geltenden zusätzlichen rechtlichen Informationen.

Wenn Sie mit diesen Nutzungsbedingungen nicht einverstanden sind, dürfen Sie auf keine weiteren Seiten der UBS-Webseite zugreifen.

auf Copyrights und andere Eigentumsrechte enthält. Es ist den Benutzern unter Anderem verboten, irgendwelche Informationen, Texte, Grafiken, Bilder, Videoclips, Verzeichnisse, Datenbanken, Listen oder Software, die von der UBS-Webseite stammen, im Ganzen oder teilweise ohne die vorherige schriftliche Genehmigung von UBS zu verändern, zu kopieren, zu senden, weiterzugeben, auszustellen, vorzuführen, zu reproduzieren, zu veröffentlichen, zu lizenzieren, als Frame in einer Webseite zu verwenden, zu übertragen und von den genannten Inhalten abgeleitete Werke zu erstellen oder sie auf andere Art für gewerbliche oder öffentliche Zwecke zu nutzen. Ohne die schriftliche Genehmigung von UBS ist es untersagt, systematisch Inhalte von der UBS-Webseite abzurufen (sei es durch Robots, Spiders, automatisiert oder manuell), um direkt oder indirekt eine Sammlung oder Datenbank oder ein Verzeichnis zusammenzustellen oder auf die UBS-Webseite zu verlinken.

## OR 1 - Vertragsschluss - Nutzungsbedingungen



### Scraping Software unzulässig

LinkedIn ist ständig bestrebt, die Daten seiner Mitglieder zu sichern und zu schützen. Damit die Daten geschützt sind, die uns unsere Mitglieder anvertrauen, erlauben wir keine Verwendung von Software Dritter, einschließlich von Webcrawlern, Bots, Browser-Plug-ins oder Browsererweiterungen (oder Add-ons), die Profile oder Kontaktinformationen auf LinkedIn scrapen oder kopieren. Diese Tools verstoßen gegen die **Nutzervereinbarung** einschließlich der in Abschnitt 8.2 aufgeführten zu unterlassenden Handlungen (ohne jedoch auf diese begrenzt zu sein):

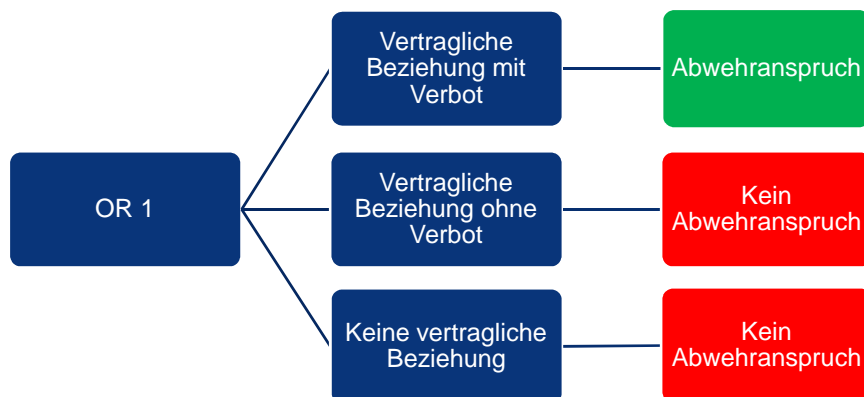
- Profile und Informationen anderer durch irgendwelche Mittel scrapen oder kopieren (einschließlich durch Webcrawler, Browser-Plug-ins und Add-ons sowie andere Techniken oder manuelle Vorgehensweisen)
- Ohne Zustimmung von LinkedIn Deep-Links zu unseren Diensten zu anderen Zwecken als zur Werbung für Ihr Profil oder eine Gruppe auf LinkedIn zu nutzen (wie in den Markenrichtlinien dargelegt)
- Die Dienste oder verbundene Technologien von LinkedIn kopieren oder modifizieren oder abgeleitete Werke davon erstellen (außer LinkedIn hat dies ausdrücklich genehmigt)
- Von LinkedIn erlangte Informationen ohne die Genehmigung von LinkedIn sammeln, verwenden, kopieren oder übertragen
- Informationen anderer Personen ohne deren ausdrückliche Genehmigung teilen oder offenlegen
- Manuelle oder automatisierte Software, Geräte, Skriptroboter oder andere Mittel oder Prozesse nutzen, um auf die Dienste oder damit verbundene Daten oder Informationen zuzugreifen, um sie zu kopieren zu „scrapen“ zu „crawlen“ oder zu „spidern“

## OR

| OR 1                        |  |  |
|-----------------------------|--|--|
| «allg. Nutzungsbedingungen» | Rein einseitige Erklärung oder konkludente Annahme | Besondere Hinweise erforderlich und hinreichend? |
| «Accept» Feld o.ä.          | Zustimmung / Vertragsschluss                       | Einwilligungserklärung durch «bot»?              |

Gegenargumente: OLG Frankfurt am Main, Urteil vom 5.3.2009, 6 U 221/08: «Wesen» einer Internetseite <-> Hausrecht: Nutzungsbedingungen und weitere einseitige Erklärungen über gewollte Nutzungsbeschränkung kommt keine Rechtswirkung zu

## OR



## DSG

| DSG 3, 12 III                              |   |   |
|--|---|---|
| Personendaten                              | Personendaten   | z.B. «local.ch»<br>Handelsregister<br>Social Media - Plattformen  |
| Rechtfertigungsgrund                       | durch betroffene Person öffentlich zugänglich gemacht (DSG 12 III)» -> «freie» Nutzung? | (sehr) zurückhaltend BVGer A-4232/2015 vom 18.4.2017 – Moneyhouse |
| Wie kann sich der Websitebetreiber wehren? |   |   |

## Ein Blick über die Grenze: DB-RL: Richtlinie 96/9/EG

| DB-RL                                 | Richtlinie 96/9/EG  |   |
|---------------------------------------|---|---|
| DB-RL 3                               | Urheberrechtlicher Schutz von Datenbank, wenn geistige Schöpfung                          |   |
| DB-RL 7                               | Sui-generis Schutz DB, wenn wesentliche Investition bei Beschaffung, Prüfung, Darstellung | Schutz nur gegen <ul style="list-style-type: none"> <li>- Entnahme/Weiterverwendung Gesamtheit oder wesentlicher Teil des Inhalts</li> <li>- Wiederholte und systematische Entnahme/Weiterverwendung, wenn unzumutbare Beeinträchtigung der Interessen des Herstellers oder normaler Nutzung entgegenstehend</li> </ul> |
| DB-RL 8 / 15                          | Keine weitergehende (vertragliche) Beschränkung   | - «normale Benutzung» erlaubt   |
| EuGH vom 15.1.2015, C-30/14 - Ryanair | DB, die weder unter DB-RL 3 noch 7 geschützt  | - Kein Schutz<br>- Kein Verbot vertraglicher Einschränkungen  |

## Ein Blick über die Grenze – BGH, Urteil v. 30.04.2014, Az. I ZR 224/12 zum dUWG

Allerdings kann die Überwindung einer technischen Schutzvorrichtung, mit der ein Mitbewerber verhindert, dass sein Internetangebot von der Allgemeinheit genutzt werden kann, ein Umstand sein, der einen Unlauterkeitsvorwurf begründet. Dem liegt die Erwägung zugrunde, dass sich ein Unternehmer, der sein Angebot im Internet öffentlich zugänglich macht, im Allgemeininteresse an der Funktionsfähigkeit des Internets daran festhalten lassen muss, dass die von ihm eingestellten Informationen durch übliche Suchdienste in einem automatisierten Verfahren aufgefunden und dem Nutzer entsprechend seinen Suchbedürfnissen aufbereitet zur Verfügung gestellt werden. Er muss deshalb auch

Onlinebörse). Dagegen ist das Allgemeininteresse an der Funktionsfähigkeit des Internets dann nicht mehr betroffen, wenn der Unternehmer durch technische Maßnahmen verhindert, dass eine automatisierte Abfrage der Daten seines Internetangebots möglich ist (vgl. BGHZ 156, 1, 18 -Paperboy; BGH, GRUR 2011, 1018 Rn. 69 - Automobil-Onlinebörse; vgl. auch Deutsch, GRUR 2009, 1027, 1032).

## Ein Blick über den Teich – kreative Ideen

7  
8 UNITED STATES DISTRICT COURT  
9 NORTHERN DISTRICT OF CALIFORNIA  
10  
11 LinkedIn Corporation,  
12 Plaintiff,  
13 vs.  
14 Does, 1 through 100 inclusive,  
15 Defendants.  
16  
17  
18  
19  
20  
21

Case No. 5:16-cv-4463

**Complaint For:**  
(1) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §§ 1030 ET SEQ.;  
(2) VIOLATION OF CALIFORNIA PENAL CODE §§ 502 ET SEQ.;  
(3) VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, 17 U.S.C. §§ 1201 ET SEQ.;  
(4) BREACH OF CONTRACT;  
(5) TRESPASS; AND  
(6) MISAPPROPRIATION

**DEMAND FOR JURY TRIAL**

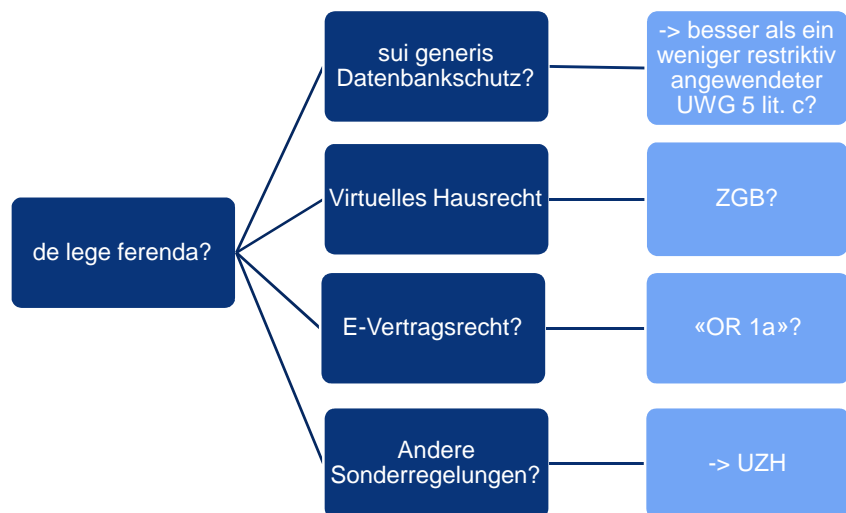
8. August 2016

## Ein Blick über den Teich – kreative «Antwort»

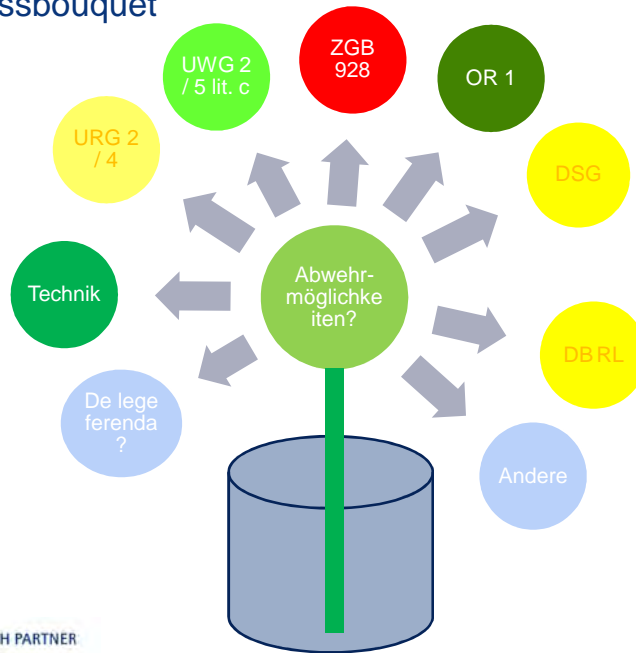


14. August 2017

## Sonderlösungen?



## Schlussbouquet

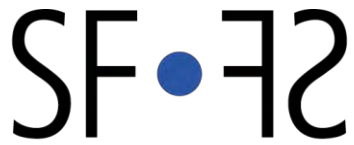


RENTSCH PARTNER AG  
Bellerivestrasse 203  
P.O. Box  
8034 Zurich  
Switzerland

[www.rentschpartner.ch](http://www.rentschpartner.ch)







Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Personal Information Management Systems (PIMS)**

CLARA-ANN GORDON





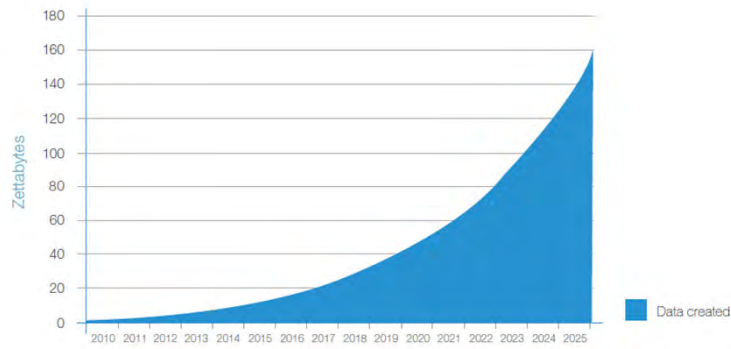
## Personal Information Management Systems (PIMS)

Dateneigentum und Datenzugang: Herausforderungen in der Praxis  
29. November 2017, 14:00 – 18:00 Uhr, Universität Zürich

## Überblick

- Einleitende Bemerkungen und Zwischenfazit
- Definitionen PIMS/PDS
- Beispiele für PIMS/PDS
- PIMS/PDS-Konzept
- Rechtslage in der Schweiz
- Massnahmenpaket der EU-Kommission zur Etablierung der «European Data Economy» vom 10. Januar 2017
- Stellungnahme des European Data Protection Supervisors
- Fazit

## Die Menge der Daten explodiert



## Was heisst Big Data?

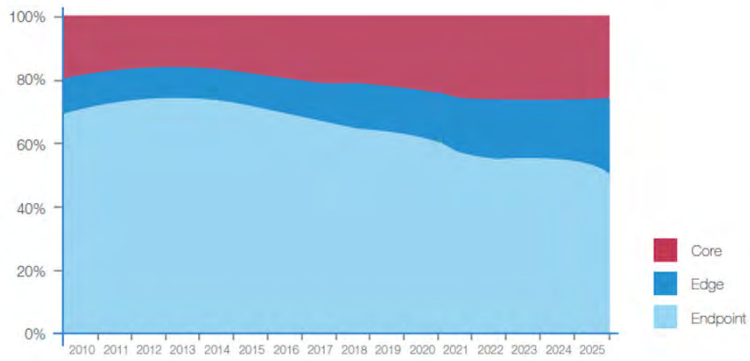
- Bit = 1 | 0
- Byte = 8 Bits
- Kilobyte (KB) = 1'000 Bytes
- Megabyte (MB) = 1'000 KB = 1'000'000 Bytes
- Gigabyte (GB) = 1'000 MB = 1'000'000'000 Bytes
- Terabyte (TB) = 1'000 GB = 1'000'000'000'000 Bytes
- Petabyte (PB) = 1'000 TB = 1'000'000'000'000'000 Bytes
- Exabyte (EB) = 1'000 PB = 1'000'000'000'000'000'000 Bytes
- Zetabyte (ZB) = 1'000 EB = 1'000'000'000'000'000'000'000 Bytes
- Yotabyte (YB) = 1'000 ZB =  $10^{24}$  Bytes
- Brontobyte (BB) = 1'000 YB =  $10^{27}$  Bytes
- GeopByte = 1'000 BB =  $10^{30}$  Bytes
- ...

**1 Gogol\* =  $10^{100}$**

\*) The term was coined in 1938 by 9-year-old Milton Sirota, nephew of American mathematician Edward Kasner (see <http://en.wikipedia.org/wiki/Gogol>)

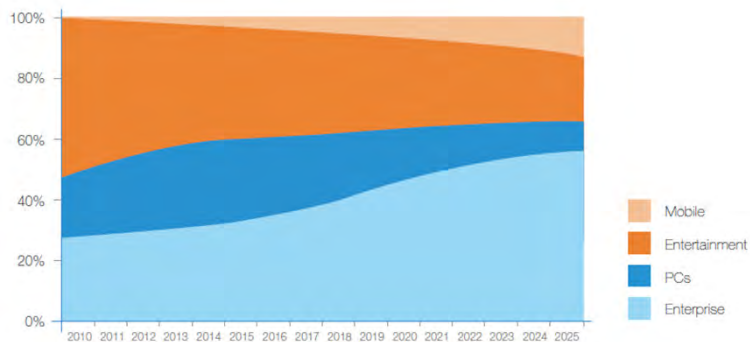
Quelle: Die Digitale Schweiz, Denkanstösse zur Datenpolitik

## Wo werden Daten generiert?



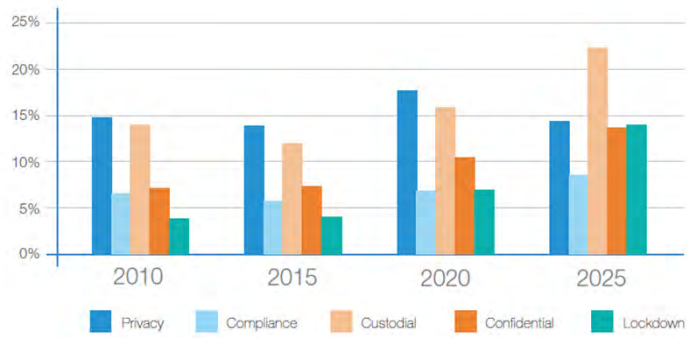
Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

## Wo werden Daten gespeichert?



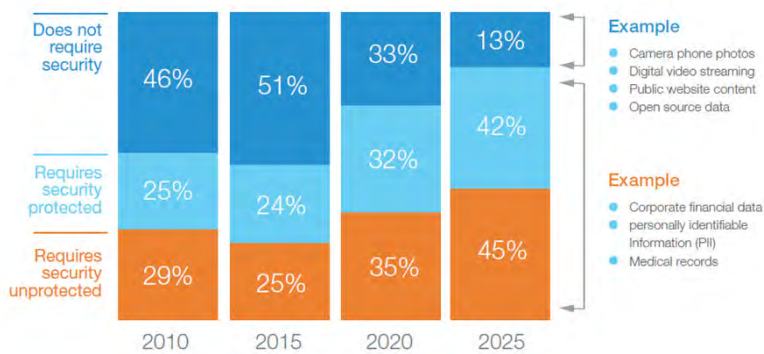
Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

## Datensicherheits- und andere Schutzanforderungen



Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

## Stand Datensicherheit



Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

## Zwischenfazit

- Datenmenge nimmt zu: 163 ZB im Jahre 2025
- Daten werden zunehmend wertvoll: «Personal Data – The New Asset Class»
- Daten fallen vor allem bei Unternehmen an und werden dort gespeichert
- Daten werden überlebensnotwendig werden (life-critical)
- Datenschutz- und Datensicherheit werden immer wichtiger und immer noch unterschätzt
- Anforderungen an Datensicherheit steigen konstant
- Ungleichgewicht zwischen Datenproduzenten- und Datenkonsumenten nimmt zu
- Forderungen der Datenproduzenten nach Selbstbestimmung werden laut
- Folge: Bewegungen und Befürworter von PIMS/PDS und Open Data

## Definitionen: PIMS/PDS

- **Personal Information Management-Systeme** (kurz «PIMS») sind Systeme, die natürlichen Personen mehr Kontrolle über ihre personenbezogenen Daten geben sollen. Mittels PIMS haben Menschen die Möglichkeit, ihre personenbezogenen Daten in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wann und mit wem sie es wünschen.
- **Personal Data Service** oder **Personal Data Store** (kurz «PDS») werden als Begriffe zunehmend anstelle von PIMS verwendet und beschreiben das Folgende:

*“...is a service to let an individual store, manage and deploy their key personal data in a highly secure and structured way. It gives the user a central point of control for their personal information (e.g. interests, contact information, affiliations, preferences, friends). The user's data attributes being managed by the service may be stored in a co-located repository, or they may be stored multiple external distributed repositories, or a combination of both. Attributes from a PDS may be accessed via an API. Users of the same PDS instance may be allowed to selectively share sets of attributes with other users.”*

## Beispiele für PIMS/PDS I – BitsaboutMe

<https://bitsabout.me/de/>

| Traditional Model<br>(Google, Facebook etc.)                              | BitsaboutMe   |
|---|---|
| Business model: Selling user data, the user is the product                | Business model: Service provider, enabling users to monetize their own data for a commission            |
| Privacy as after-thought  | Privacy by Design   |
| Users give away the rights on their data by signing the user agreement    | All data always belongs to the user. BitsaboutMe cannot touch, see or sell the data                     |
| Data is stored unencrypted in order to data mine and monetize it          | All data is encrypted, only the user has the key to decrypt   |
| Data is used to build user profiles which are then sold to advertisers    | Only user initiated analysis is done on the data. Profiles are curated by users and only shared by them |
| Little control over data, extracting and deleting data is made cumbersome | Full control at all times, straight forward extraction and deletion                                     |
| Data controllers bag all revenues from data sharing/selling               | Users earn revenues from sharing their data, BitsaboutMe gets a commission for the sale                 |

Quelle: BitsaboutMe – What is different compared to traditional data driven model?

## Beispiele für PIMS/PDS II – VALID

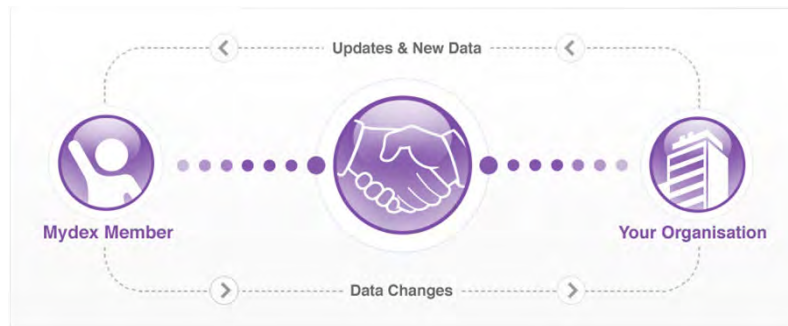
<https://procivis.ch/category/valid/>





## Beispiele PIMS/PDS III - Mydex

<https://mydex.org/>



NKF

PIMS/PDS

29. November 2017

Page 13

## PIMS/PDS-Konzept

- Neuer Ansatz dem zufolge Menschen Besitzer ihrer eigenen personenbezogenen Daten sind
- Derzeit beherrscht eine kleine Zahl von Dienst Anbietern die Landschaft von Online-Diensten den Markt und macht die personenbezogenen Daten von Nutzern als Gegenleistung für «kostenlose» Dienste zu Geld machen
- Häufig herrscht ein Machtungleichgewicht – Kunde meistens vor der Wahl «friss oder stirb»
- Kerngedanke hinter PIMS/PDS besteht darin, anbieterzentrierte System umzuwandeln und Menschen zum Management und zur Kontrolle ihrer Online-Identität zu befähigen
- Menschen sollen grundsätzlich in der Lage sein, darüber zu entscheiden, ob und mit wem, zu welchem Zweck und für welchen Zeitraum sie ihre personenbezogenen Informationen teilen möchten
- PIMS/PDS versprechen, eine neue technische Architektur und Organisation für das Datenmanagement – aus dem ein Vertrauensrahmen erwachsen soll

NKF

PIMS/PDS

29. November 2017

Page 14

## Rechtslage in der Schweiz

- Keine gesetzliche Definition von «Daten»
- Kein Eigentumsrecht an Daten
- Kein immaterialgüterrechtlicher Schutz
- Kein sui-generis Schutz für Daten
- Indirekter Schutz über UWG, StGB und andere Gesetze – aber keine Begründung eines Eigentumsrechts bzw. eines Dateneigentumsrechts
- Keine Rechtsprechung in Bezug auf Dateneigentum
- Diskussionsstand in der Literatur
- PIMS/PDS: ähnliche Situation und auch noch in den Kinderschuhen

## Bewegungen / Aktivitäten in der Schweiz

- Aktionsplan «Digitale Schweiz»:
  - Kontrolle über die eigenen Daten:

*«Im Rahmen der laufenden Revisionsarbeiten zum Datenschutzgesetz (DSG):  
Abklären der Möglichkeiten zur Umsetzung des Grundrechts auf informationelle  
Selbstbestimmung der IKT-Nutzenden, d.h. zur Erhöhung der Transparenz und  
der Kontrolle über die eigenen Daten durch die IKT-Nutzenden sowie zur  
Stärkung der Kontrollinstanzen».*
  - Stand der Arbeiten: «Abgeschlossen» - Bundesrat hat die Botschaft zum Gesetzesvorhaben am 15. September 2017 verabschiedet
- Open Data Bewegung in der Schweiz seit 2010 ([www.opendata.ch](http://www.opendata.ch))
- Swisscom neu Teil der Open Data-Community: [opendata.swisscom.com](http://opendata.swisscom.com)
- [opendata.swiss](http://opendata.swiss): Schweizer Open Government Data: kostenloses Herunterladen von Behördendaten

## Massnahmenpaket der EU-Kommission

- Economy Package II - Massnahmenpaket der Europäischen Kommission betreffend den elektronischen Datenverkehr vom 10. Januar 2017
- Ziel: Unterstützung der Digitalwirtschaft in Europa um einen einheitlichen Rechtsrahmen für den elektronischen Datenverkehr zu etablieren
- Konzepte, um die europäische Datenwirtschaft voranzubringen:
  - Abbau von Datenflusshemmnissen («Free Flow of Data»)
  - Freier Zugang zu Daten («Free Access to Data»)
  - Schutz der Privatsphäre («Respect for Private Life and Communication»)
  - Rechtssicherheit durch Verantwortlichkeit («Legal Certainty through Liability»)
  - Portabilität und Interoperabilität («Portability and Interoperability»)

## Stellungnahme 9/2016 des EDPS I

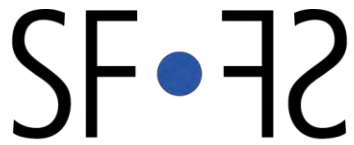
- PIMS/PDS sollen natürlichen Personen und Verbrauchern die Kontrolle über ihre personenbezogenen Daten zurückgeben
- Umwandlung von anbieterzentrierten Systemen zu menschenzentrierten Systemen
- Sicherheit und Datenschutz sind wichtigste Triebfedern für PIMS/PDS
- Nutzer sollen Möglichkeit bekommen, persönliche Analysemerkmale aufzunehmen
- PIMS/PDS unterstützen Datenschutzgrundsätze (DSGVO)
- Technische Mittel zur Einschränkung der Weiterverwendung von personenbezogenen Daten
- Transparenz und Rückverfolgbarkeit
- PIMS/PDS sind Vermittler oder Plattformen, die Verbindung zwischen den beiden Seiten des Markts fungieren: Rollen und Haftung müssen klar erläutert werden

## Stellungnahme 9/2016 des EDPS II

- Suche nach nachhaltigem Geschäftsmodell: «freemium»\_Modelle = kostenlose Basisfunktionen mit Zusatzfunktionen (z.B. kostenlose Basisfunktionen mit Zusatzfunktionen)
- Verhaltenkodizes und Zertifizierungsregelungen, wie in der DSGVO vorgesehen, werden durch PIMS/PDS unterstützt
- Schwierigkeit von PIMS/PDS sich im Markt von Online-Diensten durchzusetzen, die sich auf Geschäftsmodelle und technische Architekturen stützen, bei denen Menschen keine Kontrolle über ihre Daten haben

## Fazit

- Die flächendeckende Einführung von PIMS/PDS wäre ein Paradigmenwechsel
- Es gibt jedoch verschiedene, rechtliche Herausforderungen:
  - Diverse Zielkonflikte: Ständiges Datenwachstum vs. Datenminimierung
  - Rolle: ist ein Unternehmen noch ein Verantwortlicher (Controller), wenn die Daten beim PIMS/PDS Provider anfallen? Ist der PIMS/PDS Provider Auftragsdatenbearbeiter (Processor)?
  - Haftung: wer haftet? Verantwortlicher (Controller) und/oder PIMS/PDS Provider?
  - Unternehmen investieren Geld in die Auswertung von Rohdaten. Wird dies auch noch der Fall sein, wenn Unternehmen für die Rohdaten bezahlen müssen?
  - Etc.
- Auf der anderen Seite kann ein Unternehmen ihre datenschutzrechtlichen Pflichten an den PIMS/PDS Provider «outsourcen» und diesen vielleicht besser nachkommen?
- Für die Einführung/Durchsetzung von PIMS/PDS ist in der Schweiz per se konkret keine Gesetzesänderung notwendig. Punktuell sind wohl Gesetzesänderungen notwendig, um den im Unternehmens-Alltag ergebenden Themen gerecht zu werden



Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Verlust von Daten**

Dr. GREGOR BÜHLER



# Verlust von Daten

Veranstaltung Dateneigentum und Datenzugang:  
Herausforderungen in der Praxis

Gregor Bühler  
29. November 2017

## Was heisst: "Verlust von Daten"

- Verlust mit Fremdeinwirkung oder Fremdeffekt
- d.h. ein Verlust der (exklusiven) Kontrolle des Dateninhabers durch:
  - mutwillige Einwirkung von Dritten: **"Diebstahl"** und **"Entziehung"**
  - mutwillige Einwirkung von Berechtigten: **"Verrat"**
  - Versehen, aber mit Wahrnehmung durch Dritte: **"Verlust"**
- Nicht: Datenverlust i.S. eines versehentlichen Löschsens eigener Daten
  - nicht unbedingt ein rechtliches, sondern eher ein IT-Problem

## Überblick rechtliche Verortung

- Strafrecht
- Lauterkeitsrecht
- Datenschutzrecht
- Obligationenrecht
  
- Immaterialgüterrechtliche Aspekte bleiben vorliegend ausgeklammert

## Beispiele aus der Praxis



# Digitec-Kundendaten für Missbrauch gestohlen

*Unbefugte sind ins Netz von Digitec Galaxus eingedrungen.  
Welche Kunden vom Datenklau betroffen sind.*



«Wir haben Grund zur Annahme, dass Betrüger in den Besitz von Kontaktdaten einiger unserer Kunden gekommen sind»: Ein Digitec-Mitarbeiter stellt im Lager eine Kiste in ein Regal. (Archivbild) (Bild: Keystone)

Homburger

## Szenario "Diebstahl" (1|4)

### — Problemstellung:

- Unerlaubtes Beschaffen und Kopieren der Daten
- Verwendung für eigene, i.d.R. wirtschaftliche Zwecke
- Dateneinhaber hat typischerweise selbst noch eine Kopie der Daten  
≠ Diebstahl i.S. einer "Wegnahme" (nicht-rivalisierender Gebrauch der Daten)

### — Rechtliche Erfassung:

- **Art. 143 StGB:** Unbefugte Datenbeschaffung

*<sup>1</sup> Wer in der Absicht, sich oder einen andern **unrechtmässig zu bereichern**, sich oder einem andern elektronisch oder in vergleichbarer Weise **gespeicherte oder übermittelte Daten beschafft**, die **nicht für ihn bestimmt** und gegen seinen unbefugten Zugriff **besonders gesichert** sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.*

## Szenario "Diebstahl" (2|4)

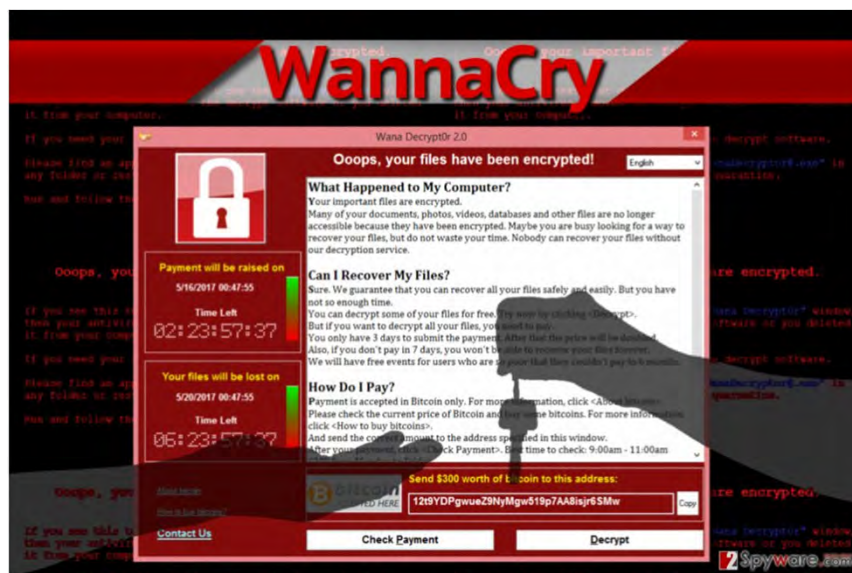
- **Art. 143<sup>bis</sup> StGB:** Unbefugtes Eindringen in ein Datenverarbeitungssystem  
*<sup>1</sup> Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
  
- **Art. 6 UWG:** Verletzung von Fabrikations- und Geschäftsgeheimnissen  
*Unlauter handelt insbesondere, wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonst wie unrechtmässig erfahren hat, verwertet oder andern mitteilt.*

## Szenario "Diebstahl" (3|4)

- **Art. 3 DSGVO:** Begriffe  
*Die folgenden Ausdrücke bedeuten:*
  - e. Bearbeiten: **jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten;**
- **Art. 4 DSGVO:** Bearbeitungsgrundsätze
- **Art. 12 DSGVO:** Persönlichkeitsverletzungen
- **Art. 13 DSGVO:** Rechtfertigungsgründe
- Abwehransprüche nach DSGVO stehen dem Datensubjekt zu (Bsp. Kunden, i.d.R. auch Opfer des Diebstahls)
  
- **Art. 41 OR:** Unerlaubte Handlung

## Szenario "Diebstahl" (4|4)

- Probleme in der Praxis:
  - *the genie is out of the bottle*-Effekt: Digitalisierung erlaubt einfaches Kopieren und globales Weiterverbreiten von beschafften Daten
  - Vorgehen gegen Dritte, die nicht selbst am "Diebstahl" beteiligt waren
  - Behauptungslast beim Geschädigten?
  - Keine Priorität bei Strafverfolgungsbehörden
  - Verfolgung zivilrechtlicher Ansprüche umständlich und risikobehaftet



## Szenario "Entziehung" (1|2)

- Problemstellung:
  - Löschung, Veränderung (z.B. Verschlüsselung) oder andere Unbrauchbarmachung der Daten
  - Dateninhaber verliert Verfügungsmacht über die Daten
  - Unter Umständen sind die Daten technisch immer noch im Einflussbereich des Dateninhabers, aber für ihn nicht mehr nutzbar (Ransomware)
  - Kopieren und Verwerten der Daten höchstens sekundär: Ransomware-Betreiber nicht unbedingt an den Daten selbst interessiert

## Szenario "Entziehung" (2|2)

- Rechtliche Erfassung:
  - **Art. 144<sup>bis</sup> StGB**: Datenbeschädigung
    - <sup>1</sup> Wer **unbefugt** elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte **Daten verändert, löscht** oder **unbrauchbar macht**, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
  - **Art. 156 StGB**: Erpressung. Wer in der **Absicht**, sich oder einen andern **unrechtmässig zu bereichern**, jemanden durch **Gewalt** oder **Androhung ernstlicher Nachteile** zu einem **Verhalten bestimmt**, wodurch dieser sich selber oder einen andern **am Vermögen schädigt**, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft
  - **Art. 41 OR**: Unerlaubte Handlung

## FINANZVERWALTUNG des Landes Nordrhein-Westfalen



MINISTERIUM DER FINANZEN



FINANZAMTSFINDER



WEITERE DIENSTSTELLEN

AKTUELLES UND PRESSE   STEUERN   FINANZEN   FINANZVERWALTUNG   SERVICE   KARRIERE

Startseite > Menü Ministerium > Aktuelles & Presse > Pressemitteilungen

### Mehr als 670 Millionen Euro für NRW

18. April 2013

## Steuer-CDs haben bisher mehr als 670 Millionen Euro für NRW gebracht

Finanzminister Norbert Walter-Borjans: "Steuerhinterzieher müssen mehr denn je damit rechnen, entdeckt zu werden."

Steuerhinterziehung, Steuerbetrug, Steuer-CD, Datenankauf

Der Ankauf von Steuer-CDs durch Nordrhein-Westfalen und die Auswertung der Selbstanzeigen haben Nordrhein-Westfalen bislang zusätzliche Einnahmen von insgesamt mehr als 670 Millionen Euro gebracht. Davon entfallen allein rund 400 Millionen Euro auf mittlerweile rund 8.000 Selbstanzeigen im Zusammenhang mit Geldanlagen in der Schweiz. Finanzminister Norbert Walter-Borjans: „Das ist Geld, das dem Gemeinwesen ohne den Kauf von Steuer-CDs vorenthalten geblieben wäre und gerade in Zeiten knapper Kassen dringend zum Beispiel für Bildung, Infrastruktur und öffentliche Sicherheit benötigt wird.“

## Fünf Jahre Haft für HSBC-Datendieb Falciani

Ehrenhafter Whistleblower oder gewissenloser Wirtschaftsspion? Das Gericht in Bellinzona konnte diese Frage im Falciani-Prozess nicht restlos klären.



Blieb der Gerichtsverhandlung fern: HSBC-Informatiker Hervé Falciani. (2. November 2015)  
Bild: Jean-Christophe Bott/Keystone

27.11.2015

**Feedback**  
Tragen Sie mit

Sein Stuhl blieb während der gesamten Verhandlung leer, einem **Urteil** konnte sich Hervé Falciani jedoch nicht entziehen. Am Freitag verurteilte das Bundesstrafgericht in Bellinzona den ehemaligen Informatiker der Bank **HSBC** zu einer Freiheitsstrafe von fünf Jahren.

## Schweiz streicht Erbe von Datendieb ein

2010 verkaufte ein Geschäftsmann Deutschland eine CD mit den Namen von Steuersündern. Doch nach seinem Freitod dürften die Erben nichts von den 2,5 Millionen Euro sehen.



2,5 Millionen Euro war dem Bundesland Nordrhein-Westfalen ein CD mit den Steuersünderwert. (Bild: Keystone/AP/Jörg Koch)

Im März vor vier Jahren verkaufte ein Geschäftsmann aus Winterthur den deutschen Behörden eine CD mit Steuersünderdaten und erhielt dafür 2,5 Millionen Euro. Ein halbes Jahr nach dem Deal wurde der 42-Jährige zusammen mit seinem Komplizen, einem Banker bei der Credit Suisse, verhaftet. Die Staatsanwaltschaft warf ihnen verbotenen Nachrichtendienst und Geldwäscherei vor. Doch zu einem Prozess gegen den Mann kam es nie. Im September 2010 nahm er sich in Untersuchungshaft das Leben.

Dossier

## Die Affäre Hildebrand

Der Wirbel um die Devisengeschäfte seiner Familie, die durch einen Datendieb publik gemacht wurden, hat Nationalbankpräsident Philipp Hildebrand zum Rücktritt bewegt. Aber auch Christoph Blocher und die «Weltwoche», die den Fall mit ins Rollen brachten, geraten unter Druck.



## Szenario "Verrat" (1|2)

Homburger

### — Problemstellung:

- Person mit Zugangsmöglichkeit kopiert Daten und gibt diese an Dritte weiter
- Musterfall: enttäuschter Arbeitnehmer ("*man with a mission*")
- Kein Eindringen in ein fremdes System notwendig
- Fragen des Vorgehens sowohl gegen den "Verräter" wie auch gegen den "Nutzniesser" des Verrats

### — Rechtliche Erfassung:

- **Art. 162 StGB** – Geschäftsgeheimnisverletzung
- **Art. 6 UWG** – Geschäftsgeheimnisverletzung
- **Art. 273 StGB** – Wirtschaftlicher Nachrichtendienst (bei Auslandsbezug)
- **Art. 320 StGB, Art. 47 BankG, Art. 35 DSG** – Amts- und Berufsgeheimnisse
- **Art. 41 OR**: Unerlaubte Handlung

## Szenario "Verrat" (2|2)

### Fälle in der Schweiz

- Steuerdaten
  - Anklage wegen Bankgeheimnis-, Geschäftsgeheimnisverletzung (Art. 47 BankG, Art. 162 StGB)
  - Verurteilung wegen wirtschaftlichem Nachrichtendienst (Art. 273 StGB)
  - Ermittlungen gegen deutsche Steuerfahnder wegen wirtschaftlichem Nachrichtendienst (Art. 273 StGB)
  - Gegenspionage (Daniel M.)
  - Einziehung von "Honorar" für Datendieb als Deliktserlös
- Affäre Hildebrand
  - IT-Mitarbeiter:
    - Bedingte Geldstrafe wegen Verletzung des Bankgeheimnisses
  - Thurgauer Anwalt:
    - Bedingte Geldstrafe wegen Gehilfenschaft zur Verletzung des Bankgeheimnisses

## Fall Peter Knäbel



### Peinlich, peinlich Frau findet HSV-Gehaltslisten im Jenischpark

09.08.15, 21:30 Uhr

EMAIL FACEBOOK TWITTER MESSENGER



The Telegraph HOME | NEWS

---

# News


---

UK | World | Politics | Budget 2017 | Science | Education | Health | Brexit | Royals

★ News

## Security breach fears over 26 million NHS patients

[share](#) [Twitter](#) [Email](#) 16



## Szenario "Verlust" (1|3) Homburger

- Problemstellung:
  - Daten gehen ohne Vorsatz verloren und werden von einem Dritten wahrgenommen
  - Daten typischerweise auf verlorenem Datenträger, aber auch andere Konstellationen denkbar (versehentliche Publikation, Upload auf öffentlich zugängliche Bereiche von Hosting-Services, unbeabsichtigter Zugang zu Datenbanken etc.)
  - Fragen des Vorgehens gegen weiterverbreitende und -verwendende Dritte

---

29. November 2017 | 20



## Szenario "Verlust" (2|3)

- Rechtliche Erfassung:
  - Schutz von Personendaten über DSGVO|ZGB
    - Verlust ist **kein** Zugänglichmachen der Daten i.S.v. Art. 12 Abs. 3 DSGVO
    - Bearbeitung kann also weiter eine Persönlichkeitsverletzung bedeuten
  - Weder Diebstahl, Entzug noch Verrat, an den (strafrechtlich) angeknüpft werden könnte
  - Eventuell Besitzschutz, falls Daten verkörpert sind

## Szenario "Verlust" (3|3)

- **Data Breach:**
  - Pflicht zur Meldung von Verletzungen der Datensicherheit, "*die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt*" (Art. 22 Entwurf revDSG)
  - Auch Verlust erfasst.
  - Konstellation: Bearbeiter verliert die Daten eines Dritten.
    - Meldung primär an EDÖB
    - Unter Umständen auch an betroffene Dritte

## Ergebnis

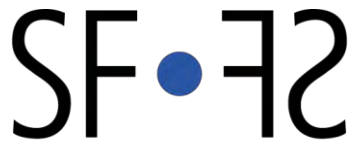
- Abwehr- und Strafinstrumente (+ kompensatorische Ansprüche)
- **Diebstahl, Entzug und Verrat** bereits heute rechtlich erfasst
  - Probleme liegen auf der Ebene der Durchsetzung
- **Verlust i.e.S.** rechtlich erfasst:
  - bei Personendaten
  - bei DatenträgernVerbesserung des Schutzes bei "anderen" Verlusten?

**Danke für Ihre Aufmerksamkeit.**

**Gregor Bühler**  
gregor.buehler@homburger.ch  
T +41 43 222 10 00

**Homburger AG**  
Prime Tower  
Hardstrasse 201  
CH-8005 Zürich

[www.homburger.ch](http://www.homburger.ch)



Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

**Daten im Konkurs**

Dr. PETER K. NEUENSCHWANDER



# DATEN IM KONKURS

Herausforderungen in der Praxis

Dr. Peter K. Neuenschwander

ITSL - Universität Zürich | 29. Nov 2017

**SN&P** Suffert  
Neuenschwander  
Partner

## AGENDA

1. EINFÜHRUNG CLOUD COMPUTING
2. ÜBERSICHT KONKURSVERFAHREN
3. PROBLEMATIK & BLICK IN DIE PRAXIS
4. LÖSUNGSANSÄTZE
5. AUSBLICK

**SN&P**

# EINFÜHRUNG CLOUD COMPUTING

Technische Kernaspekte



## EIGENER SERVER / RZ

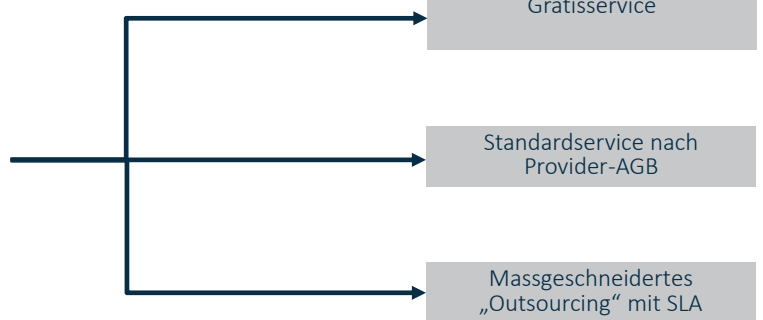
Eigene Hardware  
Definierter Standort



## CLOUD

Eigentum der Hardware?  
Speicherstandort?

Mögliche Ausprägungen:



## SPEICHERUNG / RECHENLEISTUNG ALS DIENSTLEISTUNG

- Stark abhängig von der Art des Cloud Services
- i.d.R. Fehlende Lokalisierbarkeit der Datenspeicherung auf Plattformen, die von Dritten betrieben werden

# CLOUD COMPUTING

Rechtliche Chancen und Risiken

COMPLIANCE  
THEMEN I.W.S

TECHNISCHE RISIKEN  
UND CHANCEN

RECHTLICHE RISIKEN

SICHERHEITS-RISIKEN

EFFIZIENZ  
ODER INEFFIZIENZ

ABHÄNGIGKEIT/  
LOCK-IN EFFEKT

## HAUPTTOPICS

- Datenschutz / Datensicherheit
- Eigene Handlungsfähigkeit
- Compliance mit Vorschriften allgemein

# ÜBERSICHT KONKURSVERFAHREN

Bundesgesetz über Schuldbetreibung und Konkurs (SchKG, SR 281.1)



- Betreibung / Rechtsvorschlag / Rechtsöffnung
- Fortsetzungsbegehren / Konkursbegehren
- Konkurseröffnung: Publikation im Amtsblatt

Inventaraufnahme: Konkursmasse

Einstellung mangels Aktiven

Summarisches Verfahren

- Prüfung Gläubiger-Forderung
- Kollokationsplan
- Verwertung Aktiven
- Verteilung Erlös an Gläubiger

Ordentliches Verfahren

- Gläubigerversammlung(en)
- Prüfung Gläubiger Forderung
- Kollokationsplan
- Verwertung Aktiven
- Verteilung Erlös an Gläubiger

Mangels genügender Aktiven  
→ Verlustschein

**SN&P** Suffert  
Rechtschwander  
Partner

## KONKURSMASSE – ART. 197 SCHKG



(i) Sämtliches pfändbare Vermögen, das dem Schuldner zur Zeit der Konkurseröffnung gehört, bildet, gleichviel wo es sich befindet, eine einzige Masse (Konkursmasse), die zur gemeinsamen Befriedigung der Gläubiger dient.

(ii) Vermögen, das dem Schuldner vor Schluss des Konkursverfahrens anfällt, gehört gleichfalls zur Konkursmasse.

**SN&P** Suffert  
Rechtschwander  
Partner

# ÜBERSICHT KONKURSVERFAHREN

Konkursmasse, Art. 197 SchKG



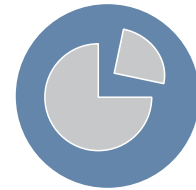
## SACHEN

Räumlich begrenzte, beherrschbare, körperliche Gegenstände



## FORDERUNGEN, DIE NICHT AUF EINE GELDLEISTUNG LAUTEN

→ Umwandlung in Geldforderung, Art. 211 SchKG



## SACHEN VON DRITTEN

→ Aussonderungsklage durch Dritteigentümer, Art. 242 SchKG



## WAS IST MIT DATEN?

auf Servern / Harddisks / in Rechenzentren / etc.

# PROBLEMATIK: DATEN IM KONKURS



## WAS IST MIT DATEN?

auf Servern / Harddisks / in Rechenzentren / etc., die im Eigentum des konkursiten Unternehmens (z.B. Cloudanbieter) stehen

## DATEN SIND KEINE SACHEN

- Daten sind keine körperlichen Gegenstände und somit im rechtlichen Sinne keine Sachen, an denen rechtliches Eigentum begründet werden kann.
- Nur körperliche Sachen können herausgegeben und im Sinne der Aussonderungsklage (Art. 242 SchKG) klageweise ausgesondert werden.



# DATEN IM KONKURS: BLICK IN DIE PRAXIS

Umfrage bei Konkursämtern (Zürich, Chur, Altdorf)



## SCHICKSAL DER DATEN IM KONKURSVERFAHREN?



**Daten nicht ungeschützt:** u.a. Datenschutzgesetz, unlauterer Wettbewerb, oder Strafrecht (Firmen- und Geschäftsgeheimnisse)



**Datensicherung und Aufbewahrung:** während gesetzlichen Aufbewahrungsfristen wegen allfälligen Folgeverfahren



**Verkauf von wertvollen , nachgefragten Datenbeständen**



**Datenvernichtung („wipen“)** vor Versilberung der Hardware



**Gesuch an das Konkursamt mit Bitte um Datenherausgabe:** pragmatisches Vorgehen, im SchKG nicht geregelt

**SN&P** Sufferl  
Neuenschwander  
Partner

# DATEN IM KONKURS: BLICK IN DIE PRAXIS

Umfrage bei Konkursämtern (Zürich, Chur, Altdorf)







## GESUCH AN DAS KONKURSAMT MIT BITTE UM DATENHERAUSGABE

- Aussonderungsklage (Art. 242 SchKG) nicht anwendbar;
- Gesuch untersteht keinen Formvorgaben;
- Mangels gesetzlicher Grundlage
  - Vorgehen im Ermessen des Konkursamts (Kulanz oder Pragmatismus);
  - Kein Anspruch auf Herausgabe;
  - Keine Fristen, allenfalls lange Wartedauern (Wochen/Monate);
- Keine/kaum Erfahrung seitens Konkursamt;
- Beizug von Experten für Datenmigration auf Kosten des Gesuchstellers.
  
- Auslandsbezug bei ausländischen Cloud-Betreibern: Vorgehen bei ausländischen Zwangsvollstreckungsverfahren unklar und Herausgabe weiter erschwert.

**SN&P** Sufferl  
Neuenschwander  
Partner




# LÖSUNGSANSÄTZE

Beschränkte Präventionsmöglichkeiten

|                            |  |   |
|----------------------------|--|---|
| RECHTLICHE<br>ÜBERLEGUNGEN | <b>VERTRÄGE</b>  <p>Vertrag mit Hosting-Anbieter über Eigentum an den Daten<br/>→ keine Rechtsicherheit gegenüber Konkursamt</p> <p><b>Pflicht zur Datenherausgabe vor Konkurseröffnung</b><br/>→ fühlt sich ein konkursiter Cloud-Provider dazu noch verpflichtet?</p> | <b>STANDORTWAHL</b>  <p>Cloud-Provider wählen, wo das Recht Datenherausgabe im Konkursfall vorgesehen ist<br/>→ z.B. Luxemburg<br/>→ Datenstandort ausserhalb der Schweiz tragbar?</p> |
|                            | <b>BACKUP THE BACKUP</b>  <p>Multi-Provider-Strategie<br/>→ unerwünschter Kostentreiber</p>   | <b>HOUSING STATT HOSTING</b>  <p>Eigene, als Eigentum markierte Datenträger bei Housing-Anbieter einbringen<br/>→ technisch und finanzieller Aufwand</p>                               |
| TECHNISCHE<br>ÜBERLEGUNGEN |  |   |

# AUSBLICK

Rechtsentwicklungen und parlamentarische Initiative

|  |   |   |  |   |   |
|--|---|---|--|---|---|
|  | <b>LUXEMBURG</b>  |  | <b>RECHTSENTWICKLUNG</b>   |  | <b>PARL. INITIATIVE</b>   |
|  | <ul style="list-style-type: none"> <li>- Gesetz mit Regelung über Vorgehen bei Insolvenz eines Besitzers fremder Daten: Anspruch auf Rück-/Übergabe von nicht-körperlichen, beweglichen Vermögenswerten</li> <li>- Voraussetzung: (i) Konkursit = Datenbesitzer (nicht aber Eigentümer), (ii) Daten anvertraut, (iii) Daten separierbar (iv) Kosten zulasten Antragsteller</li> </ul> |   | <ul style="list-style-type: none"> <li>- Revision DSG: Diskussion über Eigentumsrecht an Daten<br/>→ wird nicht umgesetzt</li> <li>- Virtuelle Währungen: Bundesrat prüft, ob Eigentum an solchen digitalen Daten begründet werden kann<br/>→ Vernehmlassungsvorlage zu Bankengesetzes und der Bankenverordnung (FinTech)</li> </ul> |   | <ul style="list-style-type: none"> <li>- <b>NR Marcel Dobler</b>, Präsident von ICTSwitzerland</li> <li>- de lege ferenda eine Erweiterung der gesetzlichen Aussonderungsrechte im Konkurs auf Daten in der Schweiz vorzunehmen.</li> <li>- Parlamentarische Initiative vom 07.03.2017,<br/><b>«Daten sind das höchste Gut privater Unternehmen: Daten-Herausgabe bei Konkurs von Providern regeln»</b></li> <li>- Im Rat noch nicht behandelt</li> </ul> |

NR DOBLER: PARLAMENTARISCHE INITIATIVE  
NR. 17.410



Ergänzung in Art. 242:

"Die Konkursverwaltung trifft eine Verfügung über die Herausgabe von nichtkörperlichen Vermögenswerten, welche von einem Dritten beansprucht werden.

Die Herausgabe setzt voraus, dass die nichtkörperlichen Vermögenswerte separiert werden können und der Antragsteller glaubhaft machen kann, dass diese dem Schuldner nur anvertraut sind.

Die anfallenden Kosten sind vom Antragsteller zu tragen."

SN&P Suffert  
Neuenschwander  
Partner

SN&P

Suffert  
Neuenschwander  
Partner

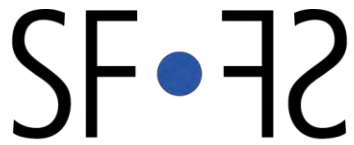


**Peter K. Neuenschwander**  
Dr. iur., IT-Rechtsanwalt

[www.snplegal.com](http://www.snplegal.com)







Schweizer Forum für  
Kommunikationsrecht



Universität  
Zürich<sup>UZH</sup>

CENTER FOR  
INFORMATION  
TECHNOLOGY  
SOCIETY AND  
LAW — ITSL

# **Dateneigentum und Datenzugang: Herausforderungen in der Praxis**

**Zürich, 29. November 2017**

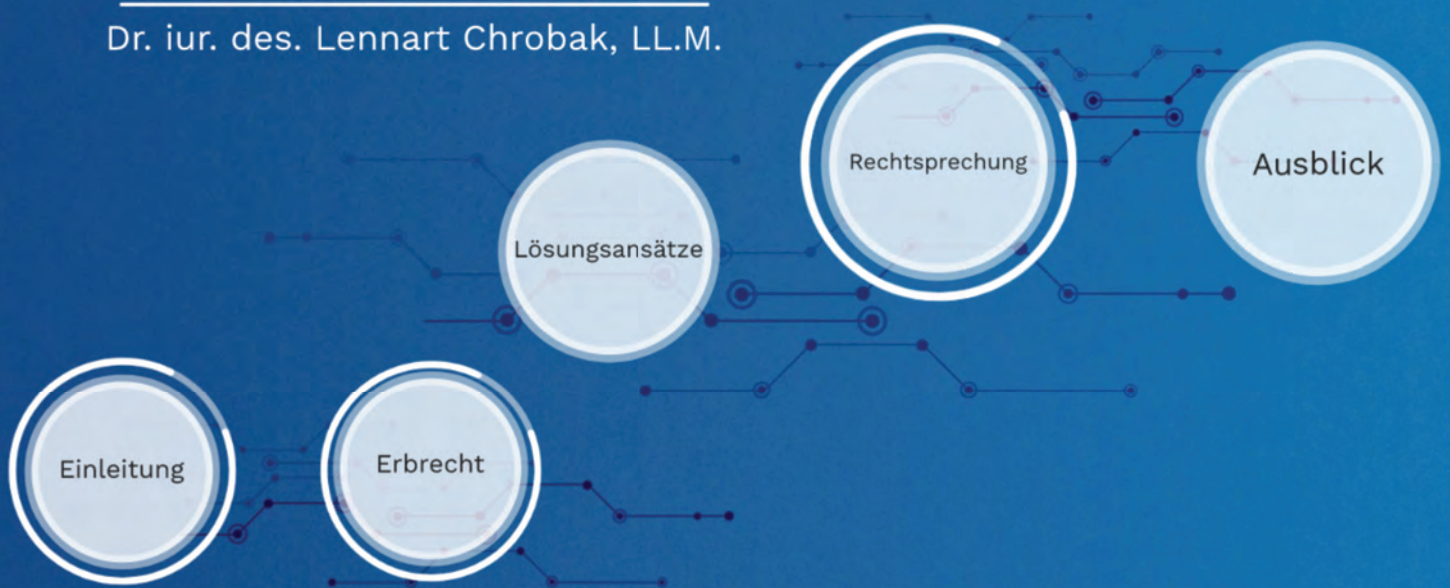
**Daten im Erbgang**

LENNART CHROBAK



# Daten im Erbgang

Dr. iur. des. Lennart Chrobak, LL.M.



## Einleitung

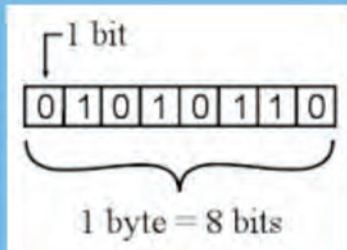
- "Digitale Daten"
- Wirtschaftliche Dimension
- Rechtliche Interdependenz

Bits & Bytes

Daten als ökonomischer Wert

Juristische Klassifikation

# Bits & Bytes



- **Information ≠ Daten**
- **Digitale und analoge Daten**
- **Lokale und Online-Daten**
- **Personen- und Sachdaten**

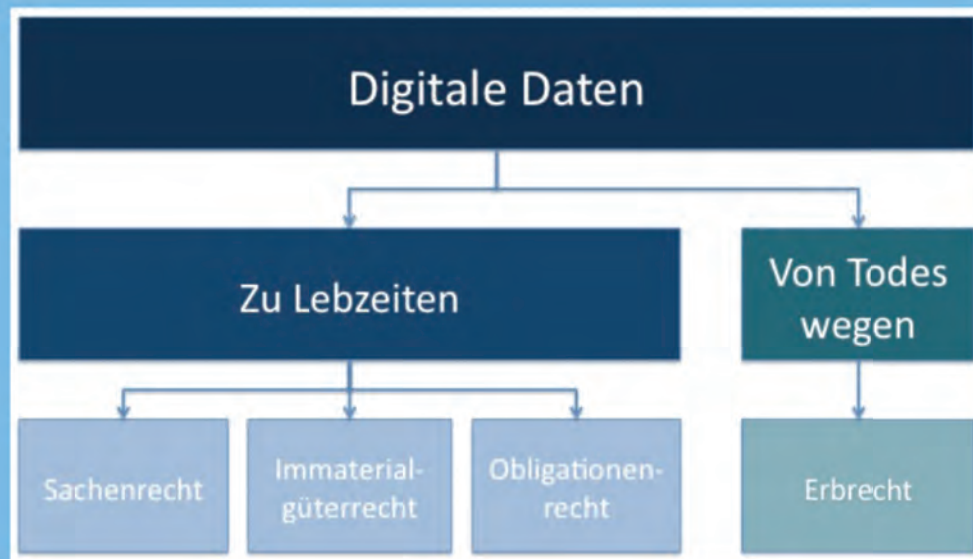
# Daten als ökonomischer Wert

- Daten als "Öl des 21. Jahrhunderts"
- Digitale und analoge Geschäftsmodelle
- Disruptive Technologien als Katalysator
- "Endowment Effect" (Richard Thaler)





# Juristische Klassifikation



## Erbrecht

Digitaler  
Nachlass

Vererbung  
von Daten

# Digitaler Nachlass

## Uneinheitliche Begriffsdefinition

- Deutscher Anwaltverein
- Uniform Fiduciary Access to Digital Assets Act (UFADAA)
- Schrifttum (z.B. Deusch)

## Hohe Diversität

- Vielzahl digitaler Nachlassgegenstände

## Werthaftigkeit des "digitalen Schattens"

- Ca. USD 35'000 (McAfee)
- Tendenz steigend





# Vererbung von Daten

## • Daten = Nachlass?

- Universalsukzession + eo ipso-Erwerb (Art. 537, 560 Abs. 1 ZGB)
- Interdependenz zur lebzeitigen Rechtslage (Art. 560 Abs. 2 ZGB)

## • Beispiele:

- => Eigentumsrechte (lokale Daten) 
- => Vertragsbeziehungen 
- => Immaterialgüterrechtsschutz (z.B. Avatar)
- => Andere digitale Daten?





# Erweiterung des Nachlassbegriffs

- **Digitale Güter als "Nachlass" i.S.v. Art. 560 Abs. 2 ZGB?**
- **Gemäss h.L. nur Eigentumsrechte an körperlichen "Sachen"**
- **Digitale Daten = "res digitalis" (vgl. Art. 713 ZGB)?**
  - Spezialitätsprinzip?
  - Publizitätsprinzip?

# Selbstregulierung der OSPs

## Google

- Kontoinaktivität-Manager
- Umfassende Lösung



## Facebook

- Nachlasskontakt
- Beschränkte Zugriffsrechte

facebook

## Dropbox

- Keine Regelung



# Digitale Nachlassplanung

## • Verfügungen von Todes wegen

- Analog
- Digital?



## • Willensvollstreckung (Art. 517 f. ZGB)

- Natürliche Personen
- Online-Dienste?



## • Digitale Vererbungsdienste

- Secure Safe (Kantonalbanken)
- UBS Safe-App (UBS)
- Legacy Locker



## Rechtsprechung

LG Berlin,  
17.12.2015 -  
20 O 172/15

KG Berlin,  
31.5.2017 -  
21 U 9/16

### LG Berlin, 17.12.2015 - 20 O 172/15



- **Zugang der Erbengemeinschaft (Mutter+Vater) zum Facebook-Konto der 15-jährigen Tochter?**
- **Erfolgslose Aufforderung zur Entsperrung des Kontos bzw. Aufhebung des "Gedenkzustandes"**
- **Klage der Eltern**
  - Vollständiger Zugang zu Konto + allen Kommunikationsinhalten
- **Urteil**
  - Vollständiger Zugangsanspruch bestätigt!
  - Gesamtrechtsnachfolge (§ 1922 BGB) umfasst Nutzungsvertrag
  - Kein Unterschied: höchstpersönl. + vermögensrechtl. Gegenstände
  - Kein Hindernis: Fernmeldegeheimnis (§ 88 TKG) + Datenschutz (BDSG)

# KG Berlin, 31.5.2017 - 21 U 9/16



- **Facebook erhebt Berufung vor KG Berlin**
- **Begründung: Fehlerhafte Würdigung der Sach-/Rechtslage**
- **Urteil**
  - Gutheissung der Berufung!
  - Offengelassen: erbrechtlicher Anspruch auf Zugang zum Nutzerkonto
  - Zugang der Erben verstösst gegen Telekommunikationsgeheimnis  
=> Verletzung der Rechte der Kommunikationspartner (Art. 88 TKG)
- **Revision beim BGH (III ZR 183/17) anhängig**

## Ausblick

Europäische  
Union

Frankreich

Schweiz

Virtual  
Property &  
Blockchain

# Europäische Union



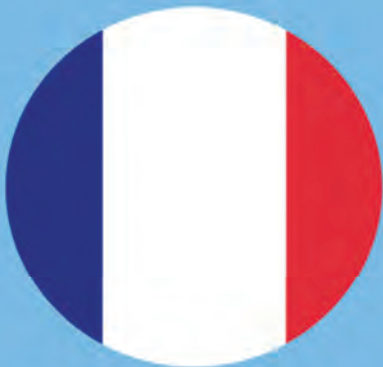
## Institut der Datenportabilität

- Art. 21 DSGVO
- VO 2017/1128/EC

## Sekundärrechtliche Harmonisierung

- US-UFADAA als Vorbild?
- EU-Kompetenz (Art. 345 AEUV)?
- Heterogenität der MS als Hindernis

# Frankreich



## Révision de la Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés

## Loi n° 2016-1321 pour une République numérique (2016)

### Art. 32

I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;

# Schweiz



- **Postulat Schwaab (14.3782/2014)**

- Richtlinien für den "digitalen Tod"

- Ergänzung des schweizerischen Erbrechts, "um die Rechte der Erbinnen und Erben auf Personendaten und digitale Zugänge der verstorbenen Person sowie um die Auswirkungen des Todes auf deren virtuelle Präsenz zu regeln."

- Annahme durch Bundes- und Nationalrat (2014)

- **Art. 16 E-DSG**

- Kostenloses Einsichtsrecht in Daten des Verstorbenen
- Erben/Willensvollstrecker können Löschung von Erblasserdaten verlangen
- Verweis auf hängige Erbrechtsrevision

# Virtual Property & Blockchain

- **"Virtual Property Rights"**

- Neuartige Rechtspositionen an Daten
- Vorbild Asien (China & Taiwan)
- Numerus Clausus dinglicher Rechte?

- **Blockchain**

- Dezentrales, beständiges Verzeichnis netzwerkinterner Datentransaktionen
- Bitcoin, Finanzdienstleistungen und Corporate Governance
- Datenzuordnung & Datenvererbung?

