Amédéo Wermelinger
Kanzlei am Bahnhof

Vertrauen durch Verträge

17. Symposium
on Privacy and Security
29. August 2012

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Dank!

Mein Dank geht an Herrn **Wolfgang Sidler**, Informatikunternehmer, vormaliger Präsident von Infosurance und Mitarbeiter des Datenschutzbeauftragten des Kantons Luzern, für seine Inputs und Unterstützung.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Agenda

- Vertrag und Vertrauen
- Vertrag und Outsourcing
- Vertrag und Cloud Comuputing
- AGB Kanton Zürich
- Folgerungen

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

1.

Vertrag und Vertrauen

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Ausgangslage

Wenn man einem Menschen trauen kann, erübrigt sich ein Vertrag. Wenn man ihm nicht trauen kann, ist ein Vertrag überflüssig.

Jean Paul Getty

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Basis des Vertrauens

- Damit Vertrauen in einen Vertrag möglich ist, gelten mindestens **3 Voraussetzungen**:
  - Die Parteien müssen vertrauenswürdig sein.
  - Die vertragliche Regelung muss verständlich sein.
  - Der Vertrag muss rechtsgültig sein.
- Diese banalen Voraussetzungen sind nicht einfach zu erfüllen.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Vertrauenswürdigkeit

- Der Laie muss sich seinen **Dienstleister sorgfältig auswählen**, da er ihm in vielerlei (technischer) Hinsicht «ausgeliefert» ist (persönliche Kenntnis der Bezugsperson von Vorteil).
- Der Auftraggeber muss sich bei **globalen Dienstleistern** (Google, Microsoft, Facebook usw.) fragen, ob ein solcher die notwendigen Voraussetzungen der Vertrauenswürdigkeit überhaupt erfüllen kann.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Verständliche Regelung I

- «Think global, act local», and rule understandable?
- Wie regelt man die Komplexität einfach?
- «Alles was einfach ist, ist falsch. Alles was komplex ist, ist unbrauchbar».

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Verständliche Regelung II

Tipps **bei Laien als Vertragspartner**:

- Keine vorgefassten «Bücher» mit allgemeinen Bestimmungen
- So **wenig Fremdwörter** wie möglich
- **Keine «Internetübersetzungen»**
- So wenig **Fachbegriffe** wie möglich (nur notorisch bekannte Fachwörter)

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Grundprobleme rechtlich I

- **Alles kann man nicht regeln**.
- Ein Vertragsverhältnis kann **nicht nur** auf der **Basis** von **Vertrauen** aufgebaut sein.
- Wenn **Kontrollmechanismen** eingeführt werden, **müssen** sie auch **eingesetzt werden**.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Grundprobleme rechtlich II

- Nicht alles, was technisch möglich ist, kann in eine (privat- oder öffentlich-rechtlich) zulässige Lösung gegossen werden: anders formuliert **geht zwingendes Recht der technischen Machbarkeit vor**.
- Es gibt Verantwortungen im (Geschäfts-)Leben, denen man sich nicht entziehen kann und die man **nicht «an die Informatik» delegieren** kann:
  - Berufsgeheimnisse
  - Haftpflicht (inkl. Produkthaftpflicht)
  - Höchstpersönliche Erfüllungspflichten

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Lösungsansätze allgemein

- Überprüfen, ob es für die zu regelnde Situation **Empfehlungen** von «neutralen» Organisationen gibt (z.B. BSI, ISO, Best Practice, Standards, usw.)
- Bei der Übernahme von Standardregeln **= zwei Fehler vermeiden**:
  - Nie übernehmen, ohne zu überprüfen, ob es passt.
  - Nie abändern, ohne zu überprüfen, welche Folgen es auf andere Bestimmungen hat.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Grundproblem technische Komplexität

- Wer nicht versteht, was er/sie macht, hat ein Problem (**Komplexität reduzieren**, wenn möglich).
- Vertragliche Regelungen sind **keine Freipässe für Unwissen**.
- Ungleichgewicht zwischen dem Erbringer von Informatikleistungen (Profi) und dem Vertragspartner (Laie); oft ist **Glossar zwingend**.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Reminder Vertragspunkte I

- **Klare Leistungsumschreibung**: Viele Verträge sind mangelhaft, weil sie nicht genau sagen, was Vertragsgegenstand und –inhalt ist.
- Klare Festlegung von **preislichen Kriterien** (insbesondere Bestellungsänderungen): Viele Vertragsbeziehungen in der Informatik werden streitig, weil ein höherer Preis als vereinbart in Rechnung gestellt wird! (Change Management, Änderungen am Lieferumfang müssen von beiden Parteien früh genug akzeptiert werden)

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Reminder Vertragspunkte II

- Klare Festlegung von **zeitlichen Kriterien**: Wann muss was erledigt sein und was geschieht, wenn nicht? (Projektmanagement)
- Klare Festlegung der **Spezifikationen**: Was muss wie gekonnt werden? Was wenn eine vereinbarte Funktionalität nicht funktioniert? (Requirements Engineering) http://de.wikipedia.org/wiki/Anforderungserhebung

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Vertrauenskiller I

- Versprochene Funktionalitäten werden nicht erreicht (es wurde **zu viel versprochen**).
- **Fristen** werden «ohne Vorwarnung» nicht eingehalten (Kunde immer über den Ablauf und über Schwierigkeiten informiert halten; Projekt-Meilensteine und Lieferergebnisse).
- Die **Kommunikation** ist ungenügend (starker Einbezug des Kunden vertraglich sichern; aber auch: Mitwirkungspflicht des Kunden festlegen).

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Vertrauenskiller II

- Die **Faktura** entspricht nicht dem Angebot.
  - Mehrbestellungen immer schriftlich vereinbaren.
  - Nicht bestellte bessere Funktionalitäten dürfen – ohne entsprechende Vereinbarung – nicht in Rechnung gestellt werden.
  - Pauschale Abmachungen respektieren.
- Die vereinbarten **Ressourcen** werden nicht zur Verfügung gestellt (Seitens Kunde oder Dienstleister) → Projektmanagement.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Bei bedeutenden Verträgen

- Immer einen **SLA** (Service-Level-Agreement) vereinbaren (kann auch in den Vertrag einfliessen bzw. als AGB ausgestaltet werden), der auch messbare Aufträge festlegt. Dazu gibt es genügend Muster und Beispiele in der Praxis.
- Bestehende Beispiele als Check-List **verwenden und kritisch hinterfragen**.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Spruch II

Ein Mann kann nie zu vorsichtig in der Wahl seiner Feinde sein.

Oscar Wilde

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

2.

Vertrag und Outsourcing

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Outsourcing in der Informatik

- **Grundsätzlich**: Auslagerung von Leistungen im Bereich der Informatik (z.B. Hardware, Software, Datenbestände) an Dritte
- **Problematik**: Ist der der Dritte vertrauenswürdig?
- Kann rechtliche Fragen aufwerfen (z.B. **Datenübermittlung ins Ausland**)

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Zulässigkeit

- Outsourcing ist nicht uneingeschränkt zulässig.
- Mögliche Hindernisse: Berufsgeheimnis, Datenschutzrecht, Verwaltungsrecht.
- Bevor man auslagert, muss also die rechtliche Zulässigkeit näher untersucht werden.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Bestimmungen im Bereich des Outsourcings I

- **Beispiele im Verwaltungsrecht:**
  - Gesetz über die Auslagerung von Informatikdienstleistungen des Kantons Zürich vom 23. August 1999 (LS 172.71) *(lag beim Check-in auf)*
  - § 13 ff. Informatikgesetz des Kantons Luzern vom 7. März 2005 (SRL Nr. 26) *(lag beim Check-in auf)*

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Bestimmungen im Bereich des Outsourcings II

Art. 10a Abs. 1 und 2 DSG

[1] Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:

a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und
b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

[2] Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Datenschutz und Outsourcing I

Folgende Themen sind beim Outsourcing besonders zu beachten/regeln:

•**Verantwortlichkeiten**: Dabei kann der Kunde in der Regel die eigene Verantwortung nicht «abtreten».

•**Verfügungsmacht:** Wer kann über die zu bearbeitenden Personendaten verfügen **und** wie sind die Daten nach Vertragsauflösung zu behandeln?

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Datenschutz und Outsourcing II

- **Bearbeitung und Zweckbindung**: Soweit Personendaten Gegenstand des Vertrags sind, muss klar definiert werden, wozu und in welchem Rahmen diese bearbeitet werden.

- **Zugriffsregelung:** Es muss geklärt werden, wer (beim Auftraggeber und beim Dienstleister) unter welchen Voraussetzungen auf welche Personendaten Zugriff hat (Achtung: Hierarchie ist noch kein Zugriffsgrund!).

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Datenschutz und Outsourcing III

- **Geheimhaltung und Bekanntgaben:** Die Geheimhaltung muss vereinbart und mögliche Bekanntgaben geregelt werden.
- **Informationssicherheit:** Der Kunde muss verlangen, dass die Personendaten, welche durch die Vertragspartei bearbeitet werden, bei diesem sicher sind (technische Fragen klären, z.B. Trennung von Datenbeständen verschiedener Kunden).

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Datenschutz und Outsourcing IV

- **Kontrollrecht**: Der Kunde muss die Möglichkeit haben, die Einhaltung der Pflichten durch die Vertragspartei kontrollieren zu lassen (ext. Audit).
- **Unterauftragsverhältnisse:** Sind solche zugelassen, wenn ja, unter welchen Voraussetzungen?

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Datenschutz und Outsourcing V

- **Technische Entwicklungen:** Wie fliessen diese ein und wer kann/muss diese auslösen bzw. darüber Beschluss fassen (Innovations-Management)?
- **Ort der Datenbearbeitung**: Soweit Personen-daten bearbeitet werden, ist der Ort der Datenbearbeitung von Belang (Art. 6 DSG).

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Spruch III

In früheren Zeiten bediente man sich der Folter.
Heutzutage bedient man sich der Presse.

Oscar Wilde

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

3.

Vertrag und Cloud Computing

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Eigenart des Cloud Computings

- Es gibt **verschiedene Standorte** der Datenbearbeitung/-haltung.
- Die **örtliche Zuweisung** erfolgt in der Regel **automatisiert** (Optimierungsprozess) und ohne Eingriff des Dienstleisters/Kunden.
- **Risiko Mangelnde Transparenz**: Nicht ohne Weiteres klar, wann und wo eine Datenbearbeitung/-haltung erfolgen wird.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Vertragstypologie

- **Komplexität**: Je nach vereinbarten Dienstleistungen stehen verschiedene Verträge oder Elemente davon zur Debatte: Leihe, **Miete** (für die Datenbeherbergung), Auftrag und Werkvertrag.
- **(Vertrags-)parteien:** Im Cloud Computing ist ein Zweiparteien Verhältnis eher selten (Kunde/Cloud Nutzer/Cloud Provider).

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Anwendbares Recht

- Der Kunde muss sicherstellen, dass er die **Gesetzesbestimmungen seines Landes** (Schweiz) einhält (nicht unproblematisch!).
- Welches Recht ist auf Datenbearbeitungen/-haltungen anwendbar, die im Ausland stattfinden? Wie, wenn ein bestimmter Vorgang in **mehreren Ländern** stattfindet?
  Lösungsmöglichkeiten:
  - Datenkommunikation so planen, dass diese bei Bedarf sofort gekappt werden kann.
  - Juristische Einheiten netzwerkmässig trennen.
  - Kontrollierten Netzübergang bauen.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Technische «Eckwerte» I

- Oft kann der Cloud Nutzer (Dienstleister) **keine Gesamtverantwortung über die Cloud** (Cloud Provider) übernehmen, da verschiedene Kunden über die Cloud bedient werden.
- **Transparenz**: Oft ist für den Kunden unklar, wer Cloud Provider ist, und er weiss nicht, wo seine Daten gegenwärtig bearbeitet werden.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Technische «Eckwerte» II

- **Informationssicherheit und Kontrolle**: Oft kann der Cloud Nutzer nur Einfluss auf die eigenen Einrichtungen und Abläufe nehmen. Quid Cloud Provider?
- **Zugriff:** Oft ist nicht klar, wer, wie und wann auf die Cloud zugreifen kann (Zugriffs-Log, -Protokoll ist zwingend).

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger Kanzlei am Bahnhof

Konsequenzen

- Datenschutzrechtlich ist das Cloud Computing sehr heikel.
- **Mögliche Lösungsansätze**:
  - Umfassende Informationspflicht über Technologie und deren Weiterentwicklung,
  - restriktive Festlegung der möglichen Bearbeitungsorte,
  - Verschlüsselung der Datenbestände und –bearbeitungen,
  - Zusicherung der Portabilität und Interoperabilität verlangen.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger Kanzlei am Bahnhof

Problem

- Gordon Frazer (UK Vice President Microsoft) sagte am 28. Juni 2011 bei der Vorstellung von Office 365 sinngemäss aus, dass die bei Microsoft-Clouds bearbeiteten Daten aufgrund des **USA PATRIOT Act** nicht vor **Zugriffen der Geheimdienste** sicher seien. Microsoft könne keine Datenschutzgarantien für Daten von EU-Bürgern abgeben.
- Was für Microsoft gilt, gilt wohl auch für **alle** anderen **US-Unternehmungen**! Jedes US-Unternehmen muss z.B. bei Verschlüsselungs-Techniken den Key beim DoD (Department of Defense) hinterlegen, also hat hier auch NSA Zugang. Unternehmungen **anderer Länder**?

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Spruch IV

Eine Zigarette ist das vollendete Beispiel eines vollendeten Genusses. Sie ist köstlich und lässt einen unbefriedigt.

Oscar Wilde

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

4.

AGB Kanton Zürich

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Unterlagen

- Merkblatt DSB Kanton Zürich über Cloud Computing *(lag beim Check-in auf)*
  siehe auch https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/formulare_und_merkblaetter.html)
- Neue AGB Auslagerung Informatikleistungen *(lag beim Check-in auf)*

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Verwendung und Zweck

- Wird einem Vertrag zur Auslagerung beigelegt
- Einhaltung des kantonalen Rechts über die Auslagerung
- Unterstützung zum Vertragsschluss auch für Private (Check List)

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Inhalt

- Auslagerung ganz allgemein
- Zusätzlich: Ziff. 13 = Cloud Computing spezifische Bestimmungen
- Sprachlich und strukturell möglichst kurz und verständlich

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Spruch V

Die Revolution ist die erfolgreiche Anstrengung, eine schlechte Regierung loszuwerden und eine schlechtere zu errichten.

Oscar Wilde

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

5.

Folgerungen

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Vertrauen durch Vertrag möglich?

Ja, **ABER**:

- Es muss **etwas dafür getan** werden (klare und rechtskonforme Regelung).
- Es muss **danach gelebt** werden (Information).
- Es muss **kontrolliert** werden können (Ressourcen und Know How!).
- Und: Man braucht eine **Exit-Strategie**.

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Schranken!

- Der Kunde muss sich zunächst selbst fragen: **Darf ich** diese Dienstleistung in dieser Form **auslagern**? (keine Probleme auslagern…)
- Falls ja, **wem** darf ich es anvertrauen?
- Welche **Schranken** muss ich dabei beachten?
- **Cloud Computing** ist möglich, aber **höchst heikel** (insbesondere aber nicht nur bei US-Unternehmungen)

Amédéo Wermelinger
Postfach 516
6023 Rothenburg

Amédéo Wermelinger
Kanzlei am Bahnhof

Spruch VI

Selig jene, die nichts zu sagen haben und trotzdem Schweigen.

Oscar Wilde

Amédéo Wermelinger
Postfach 516
6023 Rothenburg