Simmons & Simmons

Simmons & Simmons Digital Day

Digitalisierung von Unternehmen – rechtliche Herausforderungen

München, 27. April 2017

Christopher Götz, LL.M.
(New York)

Simmons & Simmons

Digitalisierung im Unternehmen

- **Automatisierung von ganzen Arbeitsabläufen / Prozessen**, z.B.:
  - „Industrie 4.0“: Produktions- & Vertriebsprozesse
  - „FinTech“: Robo-Advisor, SmartContracts & Blockchain
  - „InsurTech“: Reine Online – Versicherungsmakler;

- **Nutzung der Möglichkeiten, die das Internet bietet**, z.B.:
  - Nutzung von Speicherplatz „in der Cloud“
  - Nutzung von SaaS-Tools (z.B. MS Office 365, Salesforce, Workday)
  - MooCall (IoT)

Simmons & Simmons

Rechtliche Herausforderungen

- **IT-Vertragsrecht**
- **Datenschutzrecht**
- **Recht an Unternehmensdaten**
- **IT-Sicherheit**

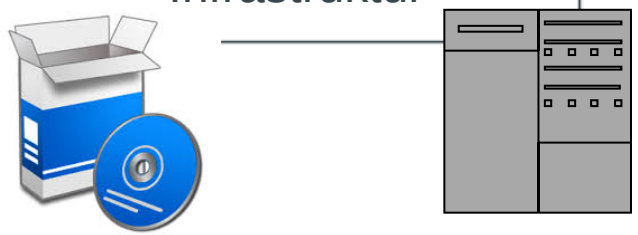
Simmons & Simmons

Rechtliche Herausforderungen

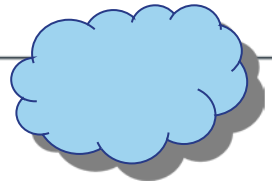
1. IT-Vertragsrecht

Moderne u. leistungsfähige IT-Systeme
zur Datenverarbeitung erforderlich

Aufbau eigener IT-Infrastruktur



Rückgriff auf Systeme Dritter



Beauftragung externer Unternehmen mit

- Aufbau der IT-Infrastruktur
- evtl. Softwareerstellung
- Wartung der IT-Systeme
- regelmäßigen Upgrades

IT-Outsourcing: Cloud Computing & Hosting durch Service Provider

- Anbindung an Internet genügt
- Skalierbarkeit

Status quo: unternehmenseigene IT - Infrastruktur

- In der Vergangenheit wurde zu wenig in IT investiert!
- ➢ Regelmäßig stark veraltete IT-Systeme (sog. „Legacy“ Systeme):
  - historisch gewachsene IT-Systeme, die sich oft auszeichnen durch
    - unzureichende Dokumentation
    - veraltete Betriebsumgebungen
    - Sicherheitslücken / Schwachstellen
  - ➢ Probleme potenzieren sich bei Fusionen von Gesellschaften

- Softwareseitig: „Open Source Software“
  - Nichteinhaltung der Lizenzbestimmungen*
  - Gefährliche Sicherheitslücken / Schwachstellen (u.a. bei Fintechs*)

* Studie „Open Source Sicherheits und Risikoanalyse 2017“ von Black Duck Software

Exemplarisch: Finanz- und Versicherungswesen

5. April 2017, 18:53 Uhr Finanzbranche

"Verheerende Befunde"

Bafin-Chef Hufeld kritisiert die Sicherheitslücken bei der IT von deutschen Banken und Versicherern.

Simmons & Simmons

IT-Vertragsrecht

- **Moderne und leistungsfähige IT-Systeme zwingend erforderlich!**
  - **Abschluss von** entsprechenden **Verträgen** mit Anbietern bzw. Service Providern erforderlich!
  - **Cloud Computing & Hosting:**
    - Werkvertrag?
    - Dienstvertrag?
    - **Mietvertrag!**

Simmons & Simmons

IT-Vertragsrecht

- **Cloud Computing & Hosting (u.a.):**
  - Verfügbarkeit
  - Back-ups (Wer? Wie oft)
  - datenschutzrechtliche Besonderheiten
    - Auftragsdatenverarbeitungsvertrag
    - Grenzüberschreitender Datentransfer
  - IT Sicherheit
  - Exit-Management
    - Was passiert mit Daten bei Vertragsablauf?

IT-Vertragsrecht

Cloud Computing & Hosting: Verfügbarkeit von Systemen

Beispiele für Verfügbarkeit („Service Level“)

Verfügbarkeit 365 Tage / Jahr 24h /Tag = 100% Verfügbarkeit	**Verfügbarkeit 99,99%**	**Verfügbarkeit 99,9 %**	**Verfügbarkeit 99,18%**	**Verfügbarkeit 91,78%**
Keine Ausfallzeit	Erlaubte Ausfallzeit: 52 Minuten pro Jahr	Erlaubte Ausfallzeit: 8H 46 Minuten pro Jahr	Erlaubte Ausfallzeit: 3 Tage pro Jahr	Erlaubte Ausfallzeit: 30 Tage pro Jahr

Simmons & Simmons

Vertragsrechtliche Besonderheiten bei IT-Outsourcing

- **Wertpapierhandelsgesellschaften / Finanzsektor / Börse**
  - Frage: Wesentliche / Unwesentliche Auslagerung?
  - ➢ Risikoanalyse!
  - ➢ "Wesentlich" → Auslagerungsvertrag:
    - Weisungsrechte, Datenschutz, Exit, IT-Sicherheit
    - **Prüfrechte BaFin / Bundesbank / EZB**

- **Versicherungen:**
  - Auslagerungsvertrag
  - Achtung bei Sparten Kranken, Unfall, Leben: § 203 Abs. 1 Nr. 6 StGB!

Aufseher fühlen der IT auf den Zahn

Welle von Sonderprüfungen – Lange Mängelliste bei Landesbanken – Strategie und Cyber-Risiken im Fokus

Die Bankenaufsicht fühlt euro- Mit einem offiziellen Bescheid rech- gerückt. Was wunder, dass die Auf-

EZB durchleuchtet IT großer Banken

Aufseher treten Welle von Prüfungen los – Notenbank besorgt

Börsen-Zeitung, 6.12.2016

bp Frankfurt Mit einer ganzen Wel fung gewesen. Im Falle der Deka- Bank trafen die Aufseher wie im Die Aufsichtsteams aus jeweils mindestens einem Vertreter der Eu

Rechtliche Herausforderungen

2. Datenschutzrecht

- Immer anwendbar wenn
  - Erhebung, Verarbeitung oder Nutzung personenbezogener Daten
    - Verarbeitung = *Übermittlung* von Daten & *Einsichtnahme*
    - Daten von Kunden, Mitarbeitern, Lieferanten (Name, Adresse etc.)
    - Eindeutige Gerätekennung
    - Dynamische IP Adresse (Breyer ./. BRD, EuGH Rs. C-582/14)
- Digitalisierung ohne „pers. Datenverarbeitung“ nicht denkbar!
- **Achtung**: pers. Datenverarbeitung nur zulässig, soweit Erlaubnistatbestand (+) oder Betroffene *wirksam* eingewilligt
- **Ausnahmen vom „Verbot mit Erlaubnisvorbehalt“?**

Datenschutzrecht

- **Konzernprivileg (-)**
- **Auftragsdatenverarbeitung**!
  - ➢ Datenübermittlung / Weiterverarbeitung iRd. ADV privilegiert, sofern

  1. *Auftragsdatenverarbeitungsvertrag*, § 11 Abs. 2 BDSG / Art 28 DSGVO
  2. Auftragnehmer = tatsächlich "verlängerter Arm" des Auftraggebers
     - vollständig weisungsgebunden!
     - kein eigenes Ermessen!
     - Problem: Tochtergesellschaft lagert bei Konzernmutter aus (HR)

Datenschutzrecht

Besonderheit: Grenzüberschreitender Datentransfer

innerhalb der EU / EWR

1. **gesetzliche Erlaubnis** oder **Einwilligung** erforderlich
   - Ausnahme: Privileg der **Auftragsdatenverarbeitung** (§ 11 BDSG / Art. 28 SGVGO)

außerhalb der EU / EWR

1. **gesetzliche Erlaubnis** bzw. **Einwilligung** erforderlich.
   - Achtung**:** auch iFd ADV!

2. **adäquates Datenschutzniveau**
   - EU – Standardvertragsklauseln

Datenschutzrecht

DSGVO ab 25. Mai 2018

ab 25. Mai 2018 ersetzt die EU-Datenschutz-Grundverordnung das BDSG und sämtliche weitere nationalen Datenschutzgesetze in EU

- Grundsatz „gesetzliche Erlaubnis oder Einwilligung“
- **Marktortprinzip** (Zielrichtung EU)!
- Privacy-by-design
- Weitergehende Dokumentationspflichten
- Datenschutzfolgenabschätzung
- Meldepflichten bei Datenpannen (72 H)

- bei Verstoß drohen Unternehmen Sanktionen von **bis zu 4%** des weltweiten Jahresumsatzes oder **EUR 20 Millionen**
- der jeweils höherer Wert ist maßgeblich

Rechtliche Herausforderungen

3. Recht an Unternehmensdaten

Möglichkeiten des Schutzes von Daten für Unternehmen?

„Eigentumsrecht“ an Daten?

- Aktuell: Nein
- ➢ Daten ≠ keine Sachen, daher eigentumsfähig (-)

Aber :

Schutz von Daten gemäß

- Vertragsrecht
- Wettbewerbsrecht
- Strafrecht
- **Datenbankrecht**

Recht an Unternehmensdaten

Datenbankrecht

„Datenbank“:

- Sammlung von bereits vorhandenen **Daten** oder „anderen unabhängigen Elementen“,
- die **systematisch** oder **methodisch** angeordnet und
- **einzeln** mit elektronischen Mitteln oder auf andere Weise **zugänglich** sind

⇨ §§ 87a ff UrhG

➢ Umfasst Daten, die **ungeordnet** auf Speichermedium abgelegt, sofern Datenbestand **mit Abfragesystem** verbunden (Indexierung)

Recht an Unternehmensdaten

Sui generis Datenbank

- Datenbank erhält **Schutz, sofern**
  - „Tätigung einer **wesentlichen Investition** in die
    - Beschaffung,
    - Überprüfung oder
    - Darstellung

    des Inhalts der Datenbank
- „Datenerzeugung selbst nicht geschützt (aber „Datengesetz“?)!
- Schutzinhaber:

  Derjenige, der das wirtschaftliche Risiko der Erstellung der Datenbank übernimmt (auch jur. Person!)

Recht an Unternehmensdaten

Schutzumfang:

- Schutz vor "**Entnahme**" oder Weiterverwendung
  - des "**gesamten Inhalts**" oder eines **"substantiellen Teils"** (qualitativ und/oder quantitativ) bzw.
  - **eines "nicht-substantiellen"** Teils, sofern
    - wiederholte und systematische „Entnahme“ und
    - keine "normale" Benutzung der Datenbank
    - keine unzumutbare Beeinträchtigung berechtigter Interessen des Datenbankherstellers
- **"Entnahme"**
  - ständige / vorübergehende Übertragung (zumindest) eines Teils des Inhalts einer Datenbank auf einen anderen Datenträger

Rechtliche Herausforderung

4. IT-Sicherheit

Wie es um das Cyber-Risk-Management derzeit bestellt ist

Obwohl die Zahl gezielter Cyber-Angriffe jährlich im zweistelligen Prozentbereich steigt, verfügt das Cyber-Management in vielen mittleren und größeren Unternehmen nicht über genügend Ressourcen.

77 % der Unternehmen verzichten auf eine Bewertung der Cyber-Risiken ihrer Lieferanten und Kunden

68 % der Unternehmen kennen die finanziellen Auswirkungen eines Cyber-Angriffs nicht

43 % der Unternehmen haben sich noch nicht mit einem sie betreffenden Cyber-Szenario beschäftigt

30 % der Unternehmen wissen noch nicht einmal im Ansatz, in welchem Maß sie Cyber-Risiken ausgesetzt sind

25 % der Unternehmen erfassen Cyber-Risiken nicht im Rahmen ihres Risikomanagements

IT-Sicherheit (exemplarisch)

IT-Sicherheit

Implementierung angemessener technischer und organisatorischer Maßnahmen

Zweck: Gewährleistung der

- **Vertraulichkeit** von Unternehmensdaten
- **Integrität** der Systeme
- dauernde **Verfügbarkeit** der Systeme

- **Vertragliche Gestaltung** (ADV)
- **Gesetze** mit Vorgaben zu IT- Standards bzw. Risikomanagementverfahren, z.B.:
  - § 9 BDSG (plus Anlage), § 11 BDSG
  - §§ 28, 32, 35, 44ff DSGVO
  - § 109 TKG (plus Katalog)
  - § 11 Abs1a EnWG (plus Katalog)
  - § 13 TMG
  - MaRisk
  - **IT-Sicherheitsgesetz**

⇨ bei Nichtumsetzung drohen V-Strafen bzw. Sanktionen durch Aufsichtsbehörde

IT Sicherheitsgesetz

IT-Sicherheitsgesetz in Kraft seit 25. Juli 2015

Inhalt:

Änderungen bestehender Gesetze:

- BSIG
- TKG
- EnWG
- TMG

Adressaten:

Betreiber *kritischer Infrastrukturen*,
§ 2 Abs. 10 BSIG

Simmons & Simmons

IT-Sicherheitsgesetz

„Kritische Infrastrukturen“ gem. § 2 Abs. 10 BSIG

Einrichtungen/Anlagen(-teile) aus folgenden Sektoren:

- Energie,
- Informationstechnik und Telekommunikation
- Transport und Verkehr,
- Gesundheit,
- Wasser,
- Ernährung oder
- Finanz- und Versicherungswesen

+

Von hoher Bedeutung für das Funktionieren des Gemeinwesens:

Ausfall/ Beeinträchtigung würde zu

- erheblichen Versorgungs-engpässen oder
- Gefährdungen für die öffentliche Sicherheit

führen.

IT-Sicherheitsgesetz

- Konkretisierung der “kritischen Infrastruktur” für oben genannte Sektoren sukzessive durch Verordnungen
- Verordnung für Sektoren **Energie, Wasser, Ernährung, Informations-technik und Telekommunikation (BSI-Kritisverordnung)**
  - Am **3. Mai 2016** in Kraft getreten
  - **Bemessungsgrundlage** für eine „kritische Infrastruktur“:
    - jeweils min. 500.000 Bürger von einer Versorgungsleistung abhängig
    - da für betroffenen Unternehmen idR unklar, ob min. 500.000 Bürger von der eigenen Leistung abhängig:
    - Einführung von messbaren Schwellenwerten (Verbrauch der Bürger wird in Schwellenwert umgerechnet)

IT-Sicherheitsgesetz

- **Messbare Schwellenwerte für Energie, Wasser, IT & TK**

  - Betreiber von *Aufbereitungsanlagen* mit einer aufbereiteten Trinkwassermenge von 22 Mio. **m³ / Jahr**;

  - Betreiber von *(Strom-)Übertragungsnetzen*, deren durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit mindestens 3.700 **GWh / Jahr** beträgt;

  - *Housing* (Betrieb eines Rechenzentrums) mit vertraglich vereinbarter Leistung von 5 **MW** (Jahresdurchschnitt)

  - *Content Delivery Networks* (z.B. MS Azure, Amazon Web Services) sofern ausgeliefertes Datenvolumen min. 75.000 **TByte / Jahr**

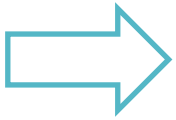
IT-Sicherheitsgesetz

- **Sektor Finanz- und Versicherungswesen**?
- Referentenentwurf des BMI (“1. Verordnung zur Änderung der BSI-Kritisverordnung”) vom 23. Februar 2017 (u.a.):
  - **Bargeldversorgung**
    - System zur Anbindung an ein Interbanken-Zahlungsverkehrsystem (Clearing und Settlement): 18 Mio dienstleistungsbez. **Transaktionen / Jahr**
  - **Kartengestützter Zahlungsverkehr**
    - Clearing und Settlement (s.o.): min. 21 Mio **Transaktionen / Jahr**
  - **Konventionellen Zahlungsverkehr**
    - Clearing und Settlement (s.o.): min. 100 Mio **Transaktionen / Jahr**

IT-Sicherheitsgesetz

- **Verrechnung und Abwicklung von Wertpapier- und Derivaten**
  - Wertpapier Clearingstelle / Settlement System: 850 000 **Transaktionen / Jahr**
  - Depotführungssystem: 850 000 **Transaktionen / Jahr**

- **Versicherungsdienstleistungen**:
  - Vertragsverwaltungssystem (Lebensversicherung): 500 000 **Leistungsfälle / Jahr**
  - Vertragsverwaltungssystem (Krankenversicherung): 2 Mio **Leistungsfälle / Jahr**
  - Vertragsverwaltungssystem (Komposit): 500 000 **Schadensfälle / Jahr**



Die Rechtsverordnung soll Ende April 2017 im Kabinett beschlossen werden.

Simmons & Simmons

IT-Sicherheitsgesetz

Verpflichtungen unter dem IT-Sicherheitsgesetz, §§ 8a, 8b BSIG

innerhalb von sechs Monaten seit Inkrafttreten der Verordnung:

- Benennung einer jederzeit erreichbaren Kontaktstelle

Achtung: keine Übergangsfrist für Energieversorger, TM-Anbieter, TK-Provider § 8c Abs. 2 und 3 BSIG

innerhalb von zwei Jahren nach Inkrafttreten der Verordnung:

- Einhaltung angemessener technischer und organisatorischer Maßnahmen zur Vermeidung von Systemstörungen
- Absicherung der Systeme nach dem „Stand der Technik“
- Nachweis durch Audits/ Zertifizierungen ggüber BSI alle 2 Jahre
- Meldepflichten im Falle von Störungen

→ Bei Verstoß: Bußgelder bis zu EUR 100.000 / Reputationsschäden!

Simmons & Simmons

Christopher Götz, LL.M. (New York)
Counsel, IT & Datenschutz
Simmons & Simmons LLP
DD +49 (0) 89 – 20 80 77 63-32
M +49 (0) 151 – 162 440 50
E christopher.goetz@simmons-simmons.com

Simmons & Simmons

simmons-simmons.com
elexica.com