Beat Lehmann, lic.iur. Fürsprech
Counsel Rio Tinto Alcan
Laurenzenvorstadt 89
Postfach 3244
5001 Aarau

Tf G: 062 - 823 29 26
Fax G: 062 - 823 29 28
E-Mail b.lehmann-aarau@bluewin.ch

^{e}CH

Rechtliche Aspekte beim Cloud Computing

I Cloud Computing aus der Sicht eines Juristen

II Wichtige Rechtsaspekte

- **Urheberrecht**
- **Datenschutzund**
- **Nachweisführung und Compliance**
- **Informatiksicherheit, Geheimhaltung**

III Vertragsnatur und Vertragsgestaltung

---

^{e}CH Abendevent
vom 9. September 2010

IBM Auditorium
Vulkanstrasse 106, Zurich-Altstetten
Donnerstag, 9. 09. 2010, 17:00 - 17:30

Grundidee

Ablösung der traditionellen Wege der Beschaffung von IT Infrastruktur und Rechnerleistungen durch Kauf / Miete / Leasing / Lizenzierung von Hardware, Software sowie Arbeitsverträge mit Mitarbeitenden durch ein umfassendes Angebot von entgeltlichen Dienstleistungen ***"Everything as a Service"***

- → PasS - **Platfom as a Service**: Bereitstellung einer Entwicklungs- und Anwendungs-Umgebung
- → SaaS - **Software-Nutzung** als Dienstleistung
- → StaaS - **Storage as a Service**: Verfügbarkeit von Speicherkapazität
- → IaaS - **IT Infrastructure als a Service**: Verfügbarkeit Recnerinfrastruktur
- → HuaaS - **Humans as a Service**: Bereitstellung menschlicher Intelligenz und Arbeitskraft für einfachere Tätigkeiten (Erkennen, Sortieren), die der Mensch noch besser erbringen kann als ein Computersystem

Vorteile für den Anwender

- → Minimale Eigen-Investitionen. Investitionen werden zu variable Kosten
- → Geringer eigener Entwicklungsaufwand
- → Man bezahlt nur, was man wirklich nutzt
- → Einmalige / seltene Anwendungen (*"high computing"*) werden bezahlbar
- → Wachsendes Angebot von Leistungen: Flexibilität
- → Dynamische Anpassung an gestiegene Bedürfnisse: Skalierbarkeit

Typische Probleme (wie bei jeder Art von Outsourcing / Offshoring)

- → Interoperabilität Abhängigkeit von Anbietern
- → Sicherheit, Vertraulichkeit, Zuverlässigkeit, Verfügbarkeit
- → Kontrollierbarkeit
- → Rückabwicklung am Vertragsende
- → **Neuartige Rechtsfragen**

Public Clouds: Gleichzeitige online Nutzung der von einem Cloud Anbieter angebotenen IT Ressourcen durch einen globalen, offenen, virtuell unbeschränkten Benützerkreis über das Internet

Community Clouds: Nutzung von IT Ressourcen durch Benutzergruppen nach mit vereibnarter Architektur, Schnittstellen, Sicheitsanforderungen

Software as a Service*
Standardprogramme zur online Nutzung durch viele Anwender auf dem System des Anbieters

Platform as a Service*
Bereitstellung einer Plattform für Entwicklung und Betrieb von Anwendungen (wie CRM, ERP) durch den Benützer, die auf einen virtuellen Server geladen wird

Storage as a Service*
Bereitstellung von virtuell unbegrenzter Kapazität zur Speicherung von Daten

Infrastructure as a Service*
Verfügbarkeit einer Umgebung von Servern mit virtuell unbegrenzter Rechnerkapazität

Humans as a Service*
über das Internet abbrufbare physische und intellektuelle menschliche Arbeitsleistung zur Ausführung einfacher Tätigkeiten": als "inkrementale Temporärabeit"

Hybride Clouds: Kombinationen von Public und Private Clouds, auch mit konventioneller IT Umgebung in Wirtschaft und Verwaltung

Private Clouds: Online Nutzung von IT Ressourcen unter eine verantwortlichen Stelle) durch einen geschlossenen Benützerkreis (Konzern, Verwaltung, Branche) über das Internet oder ein proprietäres Netzwerk

* Definitionen nach verschiedenen Angaben in der Literatur

- ❑ **Evolutionäre Weiterentwicklung** der klassischen **RZ-Lösungen** sowie des **Outsourcing** und **Offshoring** in der globalisierten Wirtschaft
- ❑ zur **universellen Verfügbarkeit** aller Informatik-Komponenten (IT Infrastruktur, Entwicklungsplattformen, Betriebs- und Anwendungs-Software)
- ❑ als **dynamisch nutzbarer Dienst**
- ❑ zugänglich über das **Internet**
- ❑ **global, ohne zeitliche und geographische Beschränkungen**
- ❑ mit **virtuell unerschöpflichen Ressourcen**
- ❑ ohne Zuweisung von Programmen, Daten, Speicherplatz, Rechnerleistung an bestimmte, geographisch lokalisierbare physische Verarbeitungsmittel
- ❑ zur **Nutzung** für eine **Vielzahl von Anwendern**
- ❑ **skalierbar** "*on demand*" nach **individuellen, wechselnden Bedürfnissen**
- ❑ unter Fakturierung eines durch **Zählung oder Messung** der tatsächlichen Nutzung ermittelten **nutzungsbezogenen Entgelts**
- ❑ mit dem **ökonomischen Effekt** der Einsparung von personellen und materiellen Investitionen in die Beschaffung und Wartung von Systemen, bzw. in die Entwicklung, Lizenzierung, sowie Betrieb, Wartung und Pflege von Betriebs- und Anwendungsprogrammen
- ❑ **und einer Anzahl neuartiger juristischer Fragestellungen**

☞ **(Haftung für) Sicherheit und Zuverlässigkeit**

Welche besonderen Risiken sind in der "Cloud" in Bezug auf RAS - Reliability, Availability, Serviceability zu beachten ?

☞ **Schutz der Geschäftsgeheimnisse**

Gefahr des Zugriffs auf vertrauliche interne Daten in der "Cloud" durch unbefugte Dritte oder ausländische staatliche Stelle; Gewährleistung und Haftung für Verlust oder Preisgabe von Daten in der Cloud

☞ **Urheberrecht**

Verfügt der Anbieter von Cloud Services über die Verwendungsbefugnisse, um Software den Anwendern über das Internet zugänglich zu machen, bzw. zur Verarbeitung von Anwenderdaten zu nutzen ?

☞ **Datenschutzrecht**

Werden beim Cloud Computing die gesetzlichen Anforderungen an den Schutz der Personendaten eingehalten ?

☞ **Compliance, Revisionsfähigkeit, Records Management**

Werden die gesetzlichen Aufbewahrungs- und Editionspflichten sowie die Anforderungen an Revisionsfähigkeit und Compliance bei der Speicherung von Geschäftsunterlagen in der "Cloud" eingehalten ?

☞ **Abhängigkeit**

Droht das Risiko der technischen, wirtschaftlichen und juristischen Bindung an den "Cloud" Service Provider bei Migraton, Restrukturierung ?

☞ **Gerichtsstand, Anwendbares Recht**

Vor welchem Gericht ("Forum") und nach welchem Recht können Ansprüche aus dem Cloud Computing geltend gemacht werden, einschliesslich (Internet) Strafrecht und Strafprozessrecht ?

☞ **Rechtsnatur des Cloud Computing und Vertragsgestaltung**

Welche besondere Anforderungen stellen sich bei der Redaktion von Verträgen mit den Anbietern von Cloud Computing Services ?

Subjektive Beurteilung * der wirtschaftlichen und juristischen Risiken beim Cloud Computing

	PaaS - Platform as-a-Service Nutzung einer An-wendungsumgebung	**SaaS** - Software as-a-Service Nutzung von Software	**IaaS** - Infrastructure / Storage as-a-Service Nutzung von Speicherplatz
Verfügbarkeit	●	●	○
Geheimhaltung	○	❑	●
Urheberrecht	○	○	❑
Datenschutz	❑	❑	●
Compliance	❑	○	●
Anwendbares Recht	○	❑	●
Vertragsgestaltung	○	❑	●

● Grosse Risiken ○ Mittlere Risiken ❑ Geringe Risiken

* Die Beurteilung nimmt auf die Erscheinungsform der Public Cloud Bezug

☞ Der Anbieter von Software in der "Cloud" muss entweder der **Inhaber** des Urheberrechts an den Programmen sein oder gemäss Art. 10 URG über die **Berechtigung** verfügen, die Programme einer Vielzahl von Benützern für den bestimmungsgemässen Gebrauch zur Verfügung zu stellen

☞ Die Klärung dieser Frage gehört zur *"due diligence"* vor dem Abschluss einer Vereinbarung über Cloud Computing für Geschäftszwecke

☞ Der Cloud.-Anbieter sollte eine entsprechende vertragliche **Rechtsgewährleistung** im Sinne von Art. 192 ff OR übernehmen

☞ Weil die Software beim Cloud Anbieter bleibt, und die mit der Programmnutzung verbundenen Vervielfältigungshandlungen durch den **Benützer** nur Schritt-für-Schritt ausgelöst, jedoch durch den Cloud Anbieter auf der bei ihm installierten Software ausgeführt werden, dürfte bei der Nutzung der Software durch den Anwender **keine Vervielfältigung oder öffentliche Verbreitung** des Programmwerks gemäss Art. 10 Abs. 2 URG iSv Art. 4 (1) (a) und (c) der Europäischen Programmschutzrichtlinie (PSRL) stattfinden

☞ Die Benützer von Software in der "Cloud" müssen daher nicht mit zivil- oder strafrechtlichen Sanktionen gemäss Art. 61 f / 71 f URG oder mit einer Beschlagnahme nach Art. 63 oder 72 URG und Art. 7 (2) PSRL rechnen

☞ Weil die Benützer der beim Aufruf des beim Cloud Anbieter gespeicherten Programme gemäss Art. 5 PSRL keine urheberechtlichen relevanten Vervielfältigungshandlungen im Sinne von Art. 4 PSRL ausführen, benötigten sie dafür weder eine Lizenz noch den Erwerb eines Programmexemplars

Richtlinie 2009/24 EG über den Rechtsschutz von Computerpgramme vom 23. April 2009
ABl L 111/16 vom 5.5.2009

☞ Weil das DSG in der Schweiz auch auf **Angaben über juristische Personen** anwendbar ist (Art. 2 Abs. 1 DSG) unterstehen die Daten über Lieferanten, Kunden oder Geschäftspartner ebenfalls dem Datenschutz

☞ Die Bearbeitung von Personendaten ist u.E. dort **unproblematisch**, wo der Benützer die Daten selber unter Benützung der in der "Cloud" zum Gebrauch beigestelltenProgramme (**SaaS**) auf seiner eigenen IT Infrastruktur bearbeitet und speichert

☞ Eine Bearbeitung von Personendaten von Benützern in der "Cloud" stellt u.E. dann **Datenschutzprobleme,** wenn Daten der Benützer auf vom Cloud Anbieter beigestellten **Infrastruktur** (IaaS) oder **Speicherplatz** (StaaS) zur Aufbewahrung von Daten in der "Cloud" bearbeitet oder speichert

☞ Das sollte für die betroffenen Personen **erkennbar** sein (Art. 4 Abs. 4 DSG), d.h. Kunden, Lieferanten, Geschäftspartner sollten z.B. durch **AGB** über die (vorgesehene) Bearbeitung ihrer Daten in der "Cloud" orientiert werden und ihr **Einverständnis** zu der damit verbundenen Bearbeitung ihrer Personendaten im Ausland erklärt haben (Art. 6 Abs. 2 (b) DSG)

☞ Es handelt sich in diesen Fällen um sog. "**Auftragsbearbeitung**"; diese ist nach Art. 10a DSG grundsätzlich **zulässig**: Der Cloud Anbieter als Auftragnehmer kann dabei die **gleichen Rechtfertigungsgründe** geltend machen, welche auch dem Benützer zustehen

☞ Dabei sich der Benützer als Auftraggeber zu vergewissern, dass der Cloud Anbieter die **Datensicherheit** gewährleistet (Art. 10a Abs. 2 DSG)

☞ Eine Bearbeitung von Personendaten im Aufttragsverhältnis kann jedoch dann unzulässig sein, wenn der Benützer **besonderen vertraglichen oder gesetzlichen Geheimhaltungspflichten** (wie das Bank- oder Arztgeheimnis) untersteht

☞ Eine **Gefährdung der Persönlichkeit** der betroffenen Personen wird dann angenommen, wenn die **Daten ins Ausland bekanntgegeben** werden und im Empfängerstaat keine Gesetzgebung besteht, die einen angemessenen Schutz gewährleistet (Art. 6 Abs. 1 DSG)

☞ Ein solcher **angemessener Datenschutz** besteht zur Zeit lediglich in den **EU-Ländern** und in wenigen Drittstaaten (Kanada, Australien, Argentinien) sowie möglicherweise dann, wenn der Cloud Anbieter unter dem mit den USA abgeschlossenen **Safe Harbor Agreement** * zertifiziert ist

☞ Eine schwerwiegende Gefährdung der Persönlichkeit tritt beim IaaS und StaaS somit dann ein, wenn sich die Personendaten des Benützers dauernd oder temporär **auf Servern** bearbeitet und/oder gespeichert werden, welche sich **in Ländern ohne angemessenen Datenschutz** befinden

☞ Darüber hinaus muss beachtet werden, dass Personendaten, welche im Ausland bearbeitet werden, dort den **Zugriffen durch die staatlichen Behörden**, auch der Fiskalbehörden, ausgesetzt sind

☞ **Datenschutzgerechte Bearbeitung von Personendaten in der "Cloud"** kann z.B. dadurch bewirkt werden, dass

- → der Datenschutz durch **Vertrag**** mit dem Cloud Anbieter gewährleistet wird (Art. 6 Abs. 2 (a) DSG)
- → der Cloud Anbieter sich verpflichtet, die Daten nur **auf Servern in Ländern mit angemessenem Datenschutz** zu bearbeiten und speichern
- → der Cloud Anbieter angemessene Massnahmen zur Datensicherung nach dem Stand der Technik anwendet (Art. 7 DSG und Art. 8-9 VDSG)
- → die Daten **verschlüsselt** bearbeitet bzw. gespeichert werden und der Schlüssel im Besitz des Benützers beibt
- → der Cloud Anbieter die verfügbaren **Rechtsmittel gegen Zugriff und Beschlagnahme** der Daten durch staatliche Behörden anwendet

* Safe Harbor Agreement EG - USA vom 27. Juli 2001; US-Swiss Safe Harbor Framework vom 9.12. 2008

** vgl. Mustervertrag des EDÖB für das Outsourcing von Datenbearbeitungen ins Ausland; EU Standardvertrag für die Übermittlung von personenbezogenen Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010

Einige Quellen von Compliance-Anforderungen

- → Ordnungsmässigkeit der "kaufmännischen Buchführung: Art. 957 ff; GeBüV und der Rechnungslegung: OR 663 a ff; Regelwerke Swiss / US GAAP - FER
- → Bestimmungen über die Rechnungslegung der Bundesverwaltung nach Art. 38 FHG iVm Art. 28, 31, 32.1 FHV
- → Einhaltung der Revisionsvorschriften von Art. 727 ff OR
- → Steuerrecht: Art. 126 DBG, Art. 57/58 MWSTG, Art. 43-45 MWSTGV, ElDI-V
- → Sozialversicherungsrecht: Art.28, 46 ATSG, Art. 67//68 AHVG, Art. 150 ff AHVV
- → Bereichsspezifische Aufbwahrungs- und Nachweispflichten, z.B.Umwelt-schutz, Verkehr mit gefährlichen Gütern, Geldwäscherei
- → Produkteischerheit, Produkthaftung, Qualitätssicherung nach DIN 9001 ff
- → Editionspflicht in Zivil-, Straf-, Verwaltungsverfahren
- → Datenschutzrecht, Wahrung der Amts- und Berufsgeheimnisse
- → Urheberrecht. Softwareschutz
- → Basel II, SOx, Gesetze über "Data Breach" und "Whistleblowing"

Wichtige Inhalte von Compliance Anforderungen

- **10 Jahre Aufbewahrung** für Geschäftsunterlagen: OR 962
- **Integrität**: Unveränderbarkeit, **Zugriffsschutz,** Art. 3, 8 und 9 GeBüV
- **Verfügbarkeit** - Art. 6 GeBüV
- Dokumentierte **Arbeitsanweisungen**: Art. 4 GeBüv; Art. 10/11 VDSG
- **Revisionsfähigkeit**: Nachprüfbarkeit, IKS OR 728a Abs. 1 Ziff. 3
- **Vorlagemöglichkeit** in ohne Hilfsmittel lesbarer Form OR 963, Art. 6 GeBüV
- **Risikobeurteilung**: OR 663b Ziff. 12

Alle diese Anforderungen an die Compliance müssen auch beim Computing in der " Cloud" erfüllt sein

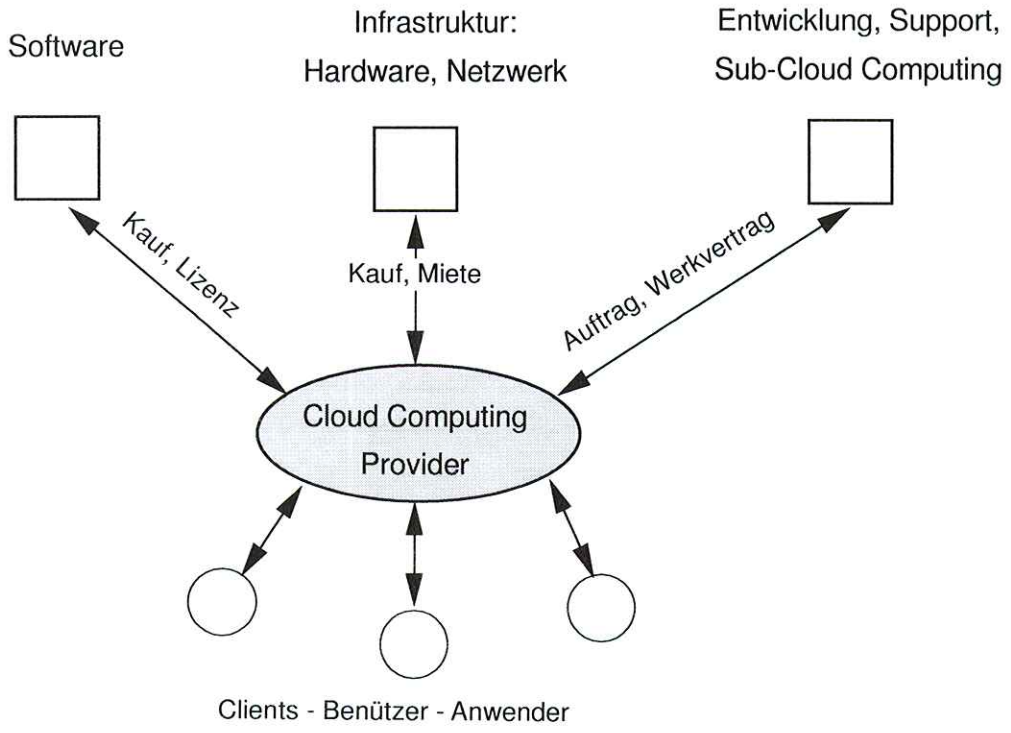
Sicherheitsrisiken beim Cloud Computing

- ❑ Verlust, Löschung, Unauffindbarkeit von Daten
- ❑ Preisgabe von Daten an die Allgemeinheit durch "*Data Breach*"
- ❑ Datenveränderung durch Schadsoftware
- ❑ Zugriffe auf Datenbestände durch Unberechtigte
- ❑ Zugang für staatliche Behörden: "Bundestrojaner"
- ❑ Minderung / Unterbruch der Verfügbarkeit
- ❑ Geschäftsaufgabe oder Konkurs des Cloud Anbieters
- ❑ Wechsel der Kontrolle über den Cloud Anbieter
- ❑ Bindung an den Cloud Anbieter; Problem der Rückabwicklung
- ❑ Verlust der Migrationsfähigkeit, Kompatibilität, Interoperabilität

Umgang mit den Sicherheitsrisiken beim Cloud Computing

- → "Due Diligence" bei Auswahl der Anwendungen und der Provider
- → Private Cloud - Proprietäre Netzwerke
- → Verschlüsselung - "Key Escrow" ?
- → Vertragliche Gewährelistungs- und Haftungs-Regelung

Struktur von Vertragsbeziehungen in der Cloud



Rechtsnatur der Verträge zwischen Cloud Anbietern und Benützern

Innominatverträge mit Elementen von

→ **Miete** (OR 253 f) / **Pacht** (OR 275 f) für den Gebrauch/Nutzung der IT- Infrastruktur: Hardware/Software/Speicherplatz

→ **Leihe** (OR 205 f) bei unentgeltlicher Nutzung der IT Resourcen

→ **Auftrag** (OR 394 f) und **Werkvertrag** (OR 363 f) für Support: Beratung, Ausbildung, resultatbezogene Dienstleistungen

Anwendbares Recht. Gerichtsstand (Forum)

- **IPR**: Recht am Sitz des Erbringers der vertragstypischen Leistung: Das ist in der Regel der Cloud Anbieter (IPRG 117)
- **Forum** an (Wohn-) Sitz des Beklagten: Art. 3 GStG/Art. 2 LugÜ, bzw. am Erfüllungsort eines Vertrages (Art. 5 Ziff. 1 LugÜ)
- **Vereinbarung** von anwendbarem Recht und Gerichsstand möglich
- Vorbehalt **zwingendes Recht**, wie DSG, Steuerecht, Buchführungsrecht

- **"Due Diligence"**: Definition der für das Cloud Computing geeigneten Anwendungen; Pflichtenheft: Zielsetzung; Mengengerüst; Anforderungen; Ausschreibung; Evaluation
- Bildung eines **"Cloud Projekt-Teams"**:Organisation; Ansprechpersonen
- Bedingungen für den Beizug von Hilfspersonen und **Unterakordanten**: "Sub Cloud Compting Provider"
- Möglichst **detaillierte Leistungsbeschreibung** in einem **SLA**: Vorgehen bei einer Erweiterung oder Reduktion der Leistungen
- Definition der **Schnittstellen** der Verantwortung und der IT Umgebung des Anwenders
- Zusicherung von **Interoperabilität** mit offenen Standards; Aufwärts-**Kompatibilität** mit der IT-Umgebung des Anwenders; **Portabilität** / und **Migrationsfähigkeit**
- Berechnung der **Vergütung**: Ansätze; Nebenkosten; Steuern, Abgaben und Gebühren; Messverfahren; Mindestabnahme ? Umsatz-Rabatte ? Anpassung / Indexierung der Vergütung ?
- **Sicherheitsanforderungen** gemäss detailliertem Handbuch
- **Verschwiegenheitspflicht** mit Pflicht zur Überbindung an Hilfspersonen und Unterakkordanten
- **Verfügbarkeitsgarantie**: Eskalationsverfahren, Notfallplanung; Back-up; Business Continuity Management; Sanktion der Nichtverfügbarkeit
- **Rechtsgewährleistung** in Bezug auf Schutzrechte Dritter
- Sorgfalt nach dem Stand der Technik
- **Gewährleistung** und (summenmässige) **Haftungsbeschränkung** bei Vertrags- und Sicherheitsverletzungen

- **Sichere Mehrfach Speicherung von Geschäftsunterlagen** während der gesetzlichen Aufbewahrungsdauer; Editionsfähigkeit
- Aufbewahrung früherer Software-Versionen zur **Gewährleistung der Revisionsfähigkeit**
- Beschränkung der **geographischen Server-Standorte**, z.B. auf den EWR; Nachweis der Safe Harbor Zertifizierung des Cloud Providers
- Projektänderungen in einem **"Change Order Procedure"**
- **Einführungs- und Betriebsunterstützung**, Ausbildung, Beratung, Hotline. Eskalationsverfahren bei Störungen
- Implementierung, **Abnahme,** Parallellauf, Beginn des vergütungs-pflichtigen Produktivbetriebes; Roll-out im Konzern
- Vorgehen bei **Auskunftsbegehren** nach dem Datenschutz
- Wahrung der Rechte des Anwenders bei **Zugriffen oder Beschlag-nahme(-Begehren)** durch Behörden und bei **e-Discovery**
- **Prüfungs- und Kontrollrechte** Rechte des Anwenders. selber oder durch beauftragte Dritte (Revisionsstelle)
- **Dauer**: Bedniungen für die Kündigung durch den Cloud Provider; ordentliche und ausserordentliche Beendigung durch den Anwender
- Vorgehen bei **Restrukturierungen** des Anwenders: Übertragung des Vertrages; Eintritt Dritter, Vorzeitige Beendigung
- **Rückabwicklung**, insbesondere Pflicht zur sofortigen und vollständigen Rückgabe aller aufgezeichneten Daten bei der Beendigung
- Schriftform für **Vertragsänderungen**
- **Anwendbares Recht, Streiterledigung, Gerichtsstand**