NÄGELE
Rechtsanwälte

27. Oktober 2016, Kommod Ruggell | RA Mag. iur. Thomas Nägele

IT-Sicherheit in Liechtenstein
Rechtliche Situation

Wer ist verantwortlich und haftet bei Schaden oder Missbrauch?

NÄGELE
Rechtsanwälte

Disclaimer

- Alle Angaben des Vortrages und dieser Präsentation erfolgen ohne Gewähr für die inhaltliche Richtigkeit und Vollständigkeit. Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers.

- Der Vortrag und die Präsentation stellen keine Rechtsberatung dar. Diese muss individuell unter Berücksichtigung der Umstände des Einzelfalls erfolgen.

NÄGELE
Rechtsanwälte

Agenda

- **Teil I - Wer haftet bei einem Hackerangriff auf die Cloud?**
  - Fallbeispiel Fitness-Center
  - Rechtliche Grundlagen / erforderliche Schutzmassnahmen
  - Allgemeine Voraussetzungen Schadenersatz
  - (Schadenersatz-)Ansprüche durch Hackerangriffe
  - Wer haftet im Unternehmen / Praxisrelevanz?

- **Teil 2 - Anforderungen an die digitale Aufbewahrung von Dokumenten**
  - Aufbewahrungspflichten im Allgemeinen
  - Anforderungen an die digitale Aufbewahrung

NÄGELE
Rechtsanwälte

Teil I

Wer haftet bei einem Hackerangriff auf die Cloud?

Fallbeispiel Fitness-Center

Daten des Fitness-Centers:

- Adressdaten (= Personendaten gemäss Datenschutzgesetz)
- Daten über Trainingsgewohnheiten
- Gesundheitsdaten (im Antragsformular, Erkrankungen)

NÄGELE
Rechtsanwälte

Das Fitness-Center wählt eine Cloud-Lösung

› Was gilt es zu beachten?

NÄGELE
Rechtsanwälte

Anwendungsbereich Datenschutzgesetz?

- Gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch Behörden und private Personen.

- Nicht für Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt.

  » Die Datenbearbeitung durch das Fitness-Center fällt unter das Datenschutzgesetz

NÄGELE
Rechtsanwälte

Personendaten (Daten)

Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen:

- z. B. Adressen (Name, Adresse, Telefon usw.)
- z. B. Arbeitsdaten (Arbeitgeber, Position, Arbeitsort)

NÄGELE
Rechtsanwälte

Besonders schützenswerte Personendaten

Daten über:

- die religiösen, weltanschaulichen und politischen Ansichten oder Tätigkeiten,
- die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe,
- administrative oder strafrechtliche Verfolgungen und Sanktionen.

» Die Datensammlung ist zum Register der Datensammlungen anzumelden

NÄGELE
Rechtsanwälte

Meldepflicht Datensammlungen

› Anmeldung zum Register der Datensammlungen: Die Anmeldepflicht zum Register der Datensammlung richtet sich nach Art. 15 DSG. Im Gegensatz zu Behörden besteht bei privaten Personen eine Anmeldepflicht nur in einem beschränkten Umfang:

› Ausgenommen von der Anmeldepflicht sind:
- Datensammlungen von Lieferanten oder Kunden, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten
- Buchhaltungsunterlagen
- Weitere Ausnahmen gemäss Art. 3a Abs. 1 Datenschutzverordnung

NÄGELE
Rechtsanwälte

Dürfen die Daten des Fitness-Centers in die Cloud?

Cloud-Dienste sind als «Auftragsdatenbearbeitung» gemäss Art. 19 Datenschutzgesetz zu qualifizieren:

- Der Auftraggeber hat dafür zu sorgen, dass die Daten nur so bearbeitet werden, **«wie er es selbst tun dürfte»** und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

- Es ist eine entsprechende vertragliche Vereinbarung (Geheimhaltungserklärung) mit dem Cloud-Service-Provider abzuschliessen.

NÄGELE
Rechtsanwälte

Inländischer / Ausländischer Cloud-Anbieter?

Zulässigkeit richtet sich nach Empfängerland:

- **EU-/EWR-Länder**
  - IdR zulässig, allgemeine Voraussetzungen sind zu beachten.
- **Drittländer mit angemessenem Datenschutz**
  - IdR zulässig, wenn Empfängerland auf der Liste der Staaten mit angemessenem Datenschutz zu finden ist (Anhang 2 Datenschutzverordnung).
  - Seit EuGH-Entscheid vom 6.10.2015 (SafeHarbor) gilt USA nicht mehr als sicher.
- **Drittländer ohne angemessenen Datenschutz**
  - Individuelle Prüfung notwendig.

NÄGELE
Rechtsanwälte

Welche Massnahmen sind zu ergreifen?

Das Datenschutzrecht verpflichtet zum Schutz von Personendaten durch «angemessene technische und organisatorische Massnahmen» gegen:

- unbefugte oder zufällige Vernichtung
- zufälligen Verlust
- technische Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen

NÄGELE
Rechtsanwälte

Technische und organisatorische Massnahmen

- Es gibt keine einheitlichen Vorgaben - die Massnahmen müssen «angemessen» sein. Die Datenschutzstelle hat Empfehlungen herausgegeben.

- Das Datenschutzrecht sieht Kriterien vor, denen Rechnung getragen werden muss (und die periodisch geprüft werden müssen):

  Zweck der Datenbearbeitung
  Art und Umfang der Datenbearbeitung
  Einschätzung der möglichen Risiken für die betroffenen Personen
  Gegenwärtiger Stand der Technik

  » Je sensibler die Daten (Gesundheitsbereich, Finanzdaten), je höher der anzuwendende Sicherheitsstandard

NÄGELE
Rechtsanwälte

Besondere Massnahmen

- Zugangskontrolle (physischer Zugang ist zu regeln)
- Personendatenträgerkontrolle (kein Zugang zu den Daten)
- Transportkontrolle (Zugang während dem Transport der Daten)
- Bekanntgabekontrolle (Identifikation der Empfänger)
- und weitere, ...

(Art. 10 Datenschutzverordnung)

NÄGELE
Rechtsanwälte

Auswahl der geeigneten Massnahmen

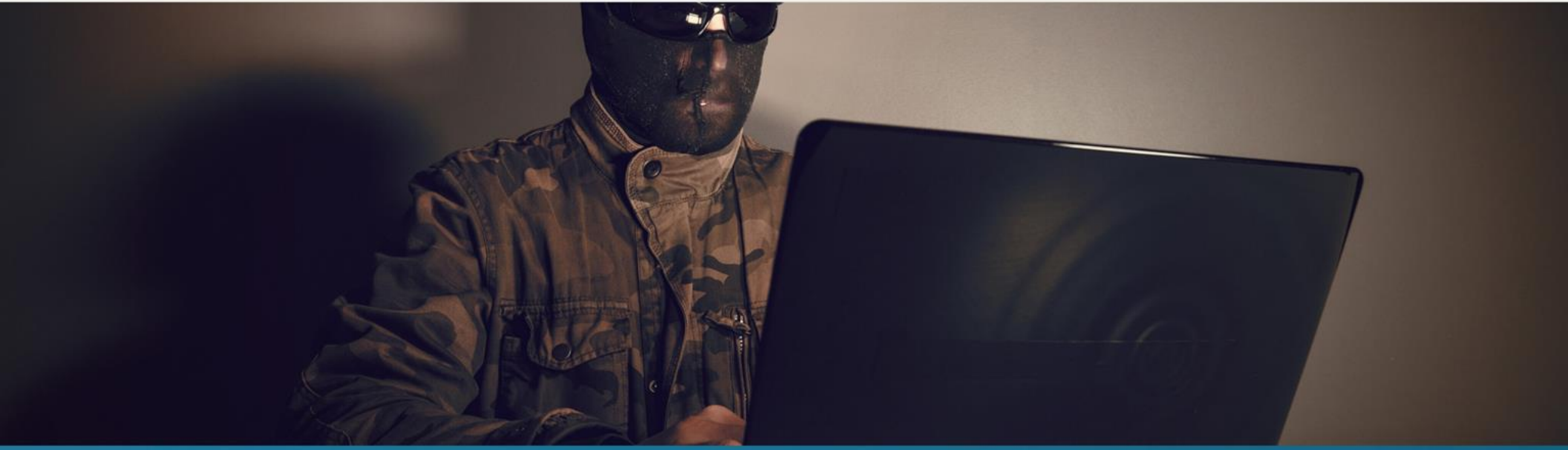
- Grundsätzlich Sache des Datenverarbeiters

NÄGELE
Rechtsanwälte

Résumé – Fitness-Center möchte in die Cloud?

- Es wurde ein liechtensteinischer Cloud-Service-Provider ausgewählt.
- Mit dem Cloud-Service- Provider wurde eine vertragliche Vereinbarung abgeschlossen und ihm darin die Pflichten nach Datenschutzgesetz für besonders schützenswerte Daten (insbesondere Geheimhaltungs-pflichten) überbunden.
- Der Cloud-Service-Provider hat die Personendaten durch angemessene technische und organisatorische Massnahmen geschützt.
- Die Datensammlung wurde zum Register der Datensammlungen angemeldet.

NÄGELE
Rechtsanwälte



Die Fitness-Center Cloud wurde gehackt

Allgemeine Voraussetzungen Schadenersatz

- Schaden
- Kausalität (Verursachung)
- Rechtswidrigkeit
- Rechtswidrigkeitszusammenhang
- Verschulden

NÄGELE
Rechtsanwälte

Haftung bei Auslagerung in die Cloud?

- Zivilrechtlich ist die Auslagerung in die Cloud eine Frage der Hilfspersonenhaftung.
- Der Auftraggeber haftet wie für eigenes Verschulden.

  » Der Cloud-Service-Provider sollte sorgfältig ausgesucht werden!

  » Für die Geltendmachung allfälliger Regressansprüche sind Cloud-Service-Provider in CH/FL/AT vorzuziehen.

NÄGELE
Rechtsanwälte

Schadenersatzansprüche der Fitness-Center Kunden?

- Der entstandene Vermögensschaden, der durch den Sicherheitsmangel entstanden ist, ist in der Praxis nur schwer zu beweisen (bspw. durch Offenlegung der politischen Gesinnung). Im Fallbeispiel muss der Schadenersatz durch Offenlegung der Gesundheitsdaten meines Erachtens an der fehlenden Kausalität scheitern.

- Wurden hingegen Finanzdaten (Kontodaten) offengelegt und damit unberechtigte Vermögenstransaktionen getätigt, ist der Schaden und die Kausalität einfacher nachweisbar.

- In Liechtenstein gibt es (noch) keine «Data Breach Notification Duty» wie in Österreich.

NÄGELE
Rechtsanwälte

Wer haftet im Unternehmen?

- IT-Sicherheit ist für die Geschäftsleitung / Verwaltung meist Sache des IT-Verantwortlichen.
- IT-Security ist aber eine Kernkompetenz eines jeden Unternehmens und somit im Verantwortungsbereich der Geschäftsleitung / Verwaltung.

  » Pflicht zur sorgfältigen Auswahl, Anleitung und Kontrolle des IT-Verantwortlichen

NÄGELE
Rechtsanwälte

Praxisrelevanz?

- In Liechtenstein soweit überblickbar keine veröffentlichen Gerichtsentscheide zum Thema.
- Bislang wird die Haftung der Geschäftsführung für Compliance-Verstösse kaum verfolgt.
- Dies kann sich angesichts des steigenden wirtschaftlichen Drucks sowie der Häufung von medial ausgeweideten Sicherheitsverstössen und öffentlich bekannten Anlassfällen rasch ändern.