Sensitive Daten und Cloud Sourcing - Rechtliche Anforderungen

Dr. iur. Jürg Schneider, Rechtsanwalt, Partner

Swiss IT Sourcing Forum, Luzern, 13. April 2016

walderwyss rechtsanwälte

Übersicht

1. Einführung in die Thematik

2. Rechtliche Anforderungen

3. Standards

4. Spezielle Themen

5. Schlussfolgerungen

1. Einführung in die Thematik

- Einige Definitionen:
  - Datenschutz
  - Informationssicherheit
  - Sensitive Daten
- Keine einzelne allumfassende rechtliche Regelung
- Spezielle Risiken: Kontrollverlust, fehlende Datentrennung, grenzüberschreitende Sachverhalte, Zugriff ausländischer Behörden, Lock-in-Effekte, Konkurs eines Cloud-Anbieters

2. Rechtliche Anforderungen (Schweiz)

- Allgemein
- Gesetzliche Regelungen
- Selbstregulierung und Softlaw
- Sarbanes-Oxley Act
- Vertragliche Anforderungen

Gesetzliche Regelungen

- Datenschutzgesetzgebung (Art. 7 DSG, Art. 8 ff. VDSG);
- Kaufmännische Rechnungslegung (Art. 957 ff. OR, Verordnung über die Führung und Aufbewahrung der Geschäftsbücher, GeBüV);
- Internes Kontrollsystem (Art. 728a Abs. 1 Ziff. 3 OR);
- Steuerrecht (z.B. Art. 70 MWStG in Verbindung mit Art. 122 – 125 MWStV sowie der Verordnung des EFD über elektronisch übermittelte Daten und Informationen);
- Geschäfts-, Amts- und Berufsgeheimnis (Art. 162 StGB, Art. 320 StGB und Art. 321 StGB);
- Sektorspezifische Regelungen (Finanzmarktgesetzgebung [z.B. FINMA-RS 2008/7 «Outsourcing Banken»; Anhang 3 FINMA-RS 2008/21 «operationelle Risiken Banken» etc.], BEHG, FinfraG).

Anforderungen aus Datenschutzgesetz (I)

- Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG) und dazugehörende Verordnung vom 14. Juni 1993 (VDSG)
- Leitfaden des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten („EDÖB“) zu den technischen und organisatorischen Massnahmen des Datenschutzes
- Leitfaden des EDÖB für die Bearbeitung von Personendaten im privaten Bereich
- Leitfaden des EDÖB für die Bearbeitung von Personendaten im Arbeitsbereich durch private Personen
- Erläuterungen des EDÖB zu Cloud Computing

Anforderungen aus Datenschutzgesetz (II)

- Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen (Art. 3 DSG).
- Anonymisierung und Verschlüsselung/Encryption
- Auslagerung der Bearbeitung an Dritte (z.B. Cloud-Anbieter) ist grundsätzlich erlaubt, sofern (Art. 10a DSG):
  - Auslagerung auf Basis eines Vertrags mit dem Cloud-Anbieter erfolgt oder gesetzlich vorgesehen ist ;
  - Personendaten nur so bearbeitet werden, wie es auch der Auftraggeber selbst tun dürfte;
  - keine **gesetzliche oder vertragliche Geheimhaltungspflicht** es verbietet; und
  - Auftraggeber sich versichert, dass Datensicherheit gewährleistet wird.
- (Schriftlicher) Vertrag (soll insbesondere auch Weisungsrechte, Bearbeitungs- und Sicherheitsinstruktionen sowie Kontrollrechte beinhalten)
- Rechtsansprüche der betroffenen Personen bei der Verletzung ihrer Persönlichkeitsrechte gegenüber Auftraggeber: Sperrung Datenbearbeitung, Berichtigung Daten, Vernichtung Daten, Schadenersatz, Genugtuung

Anforderungen aus Datenschutzgesetz (III)

- Schutzmassnahmen gegen unbefugtes Bearbeiten (Art. 7 DSG)
- Systeme müssen insbesondere gegen folgende Risiken geschützt sein: unbefugte oder zufällige Vernichtung, zufälliger Verlust, Fehler, Fälschung, Diebstahl, widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen (Art. 8 Abs. 1 VDSG).
- Schutzmassnahmen müssen angemessen sein. Kriterien sind a) Zweck der Datenbearbeitung; b) Art und Umfang der Datenbearbeitung; c) Einschätzung der Risiken für die betroffenen Personen; und d) gegenwärtiger Stand der Technik (Art. 8 Abs. 2 VDSG).
- Massnahmen sind periodisch zu überprüfen (Art. 8 Abs. 3 VDSG).
- Besondere Massnahmen bei automatisierten Bearbeitungen (Art. 9 VDSG)
- Allenfalls Pflicht zur Protokollierung der Bearbeitung und zur Erstellung eines Bearbeitungsreglements (Art. 10 und 11 VDSG)
- Gewährleistung Auskunftsrecht (Art. 8 DSG)

Anforderungen aus Datenschutzgesetz (IV)

- Wenn **Personendaten ins Ausland offenbart werden**: Sofern im Drittland für die entsprechenden Personendaten keine Gesetzgebung besteht, die einen angemessenen Schutz gewährt, und keine weiteren Ausnahmen zur Anwendung kommen, sind spezifische Datentransferverträge mit dem Cloud-Anbieter abzuschliessen und der EDÖB ist vor der ersten Offenlegung zu informieren (Art. 6 DSG).
- In der Regel werden **EU Model Klauseln** «Controller to Processor» verwendet.
- Anpassung der EU Model Klauseln auf CH-Recht?
- Achtung: EDÖB erachtet Schutz durch US-CH Safe Harbor Zertifizierung als ungenügend und hat Länderliste angepasst (indirekte Konsequenz des *Schrems Urteils* des EU-Gerichtshofs [6. Oktober 2015, Rs. C-362/14]).
- Zukünftiges «Privacy Shield»?

3. Standards

- Standards/Guidelines werden in der Praxis wichtiger.
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- SAS 70 Service Organizations / SSAE 16 Reporting Controls at a Service Organization
- Data Protection Code of Conduct for Cloud Service Providers der Cloud Select Industry Group (noch nicht final)

4. Spezielle Themen (I - Generell)

- Information der betroffenen Personen?
- Erforderlichkeit eines eigenständigen und direkten Auditrechts?
- Schicksal der Daten im Konkurs
  (Daten müssen als geheim bezeichnet werden, kein Retentionsrecht, Verwertungsverbot, nur solventer Anbieter; jedoch keine absolute Sicherheit)
- Speziell regulierte Berufe und Dienstleistungen
  (Anwälte, Ärzte, Banken, Finanzinstitute/Finanzmarktinfrastruktur etc.)
- Gruppenkonstellationen
  (parallele Anwendung verschiedener gesetzlicher / regulatorischer Anforderungen)

4. Spezielle Themen (II - Auslandsbezug)

- Zugriff auf Daten durch ausländische Behörden?
- Durchsetzbarkeit der Ansprüche im Ausland?
- EU Anforderungen:
  - Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie). **Ab ca. 2018: EU Datenschutz-Grundverordnung** (Ende April 2016 Abstimmung, dann 2 Jahre zur Umsetzung in den Mitgliedstaaten)
  - Entwurf: Data Protection Code of Conduct for Cloud Service Providers der Cloud Select Industry Group (EU-Kommission)
  - Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing of Article 29 Data Protection Working Party
  - Opinion 05/2012 on Cloud Computing of Article 29 Data Protection Working Party

5. Schlussfolgerungen (I)

- **Komplexität (und Anforderung)** steigt bei internationalen Sachverhalten.
- **Sorgfältige Auswahl** des Cloud-Anbieters
- **Legal und Business Risk Assessment**, bevor eine Cloud-Lösung gewählt wird (z.B. überprüfen, ob auf Grund von Geheimhaltungspflichten eine vorgängige Einwilligung der betroffenen Personen notwendig ist oder ob allenfalls eine vorgängige Anonymisierung in Frage kommt etc.)
- **Vertragliche Regelung** muss den rechtlichen Anforderungen Rechnung tragen (insb. folgende Punkte sind wichtig: Sicherstellung Zugriff auf eigene Daten, Dateninhaberschaft, Datentrennung, Informationspflichten, Instruktions- und Kontrollrechte, Sicherheitsvorkehrungen, Geheimhaltungspflicht, Verwertungsverbot sowie Ausschluss Retentionsrecht, Ort der Datenbearbeitung / des Datenzugriffs [allenfalls spezifische Datentransferverträge], SLAs, Beizug von Subakkordanten, Haftungsregelung, Vertragsbeendigung etc.)

5. Schlussfolgerungen (II)

- Der **Kunde ist dafür verantwortlich**, dass der Cloud-Anbieter die auf den Kunden anwendbaren rechtlichen Anforderungen einhält.
- **Informationssicherheit ist «Chefsache».**
- Bei Vernachlässigung: **Haftungs- und Reputationsrisiken**

Kontaktdetails

Walder Wyss AG
Dr. iur. Jürg Schneider
Seefeldstrasse 123
Postfach 1236
8034 Zürich
Tel. +41 58 658 55 71
Fax +41 58 658 59 59
juerg.schneider@walderwyss.com
www.walderwyss.com

Besten Dank für Ihre Aufmerksamkeit!