IT & LAW CONSULTING GMBH

Datenschutz aktuell

Themenblock 3

Grenzüberschreitender Datenverkehr und Outsourcing
in der Praxis

mag. iur. Maria Winkler, 18. März 2014

Agenda

- Datenübermittlung ins Ausland
  - Gesetzliche Grundlagen
  - US-Swiss Safe Harbor
- Outsourcing der Datenbearbeitung ins Ausland
- Cloud Computing
  - eine Qualifikation aus rechtlicher Sicht
  - wichtige Vertragspunkte zum Schutz der Daten

Grenzüberschreitende Bekanntgabe

(Art. 6 DSG)

- Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde.
- Dies ist beispielsweise der Fall, **wenn eine Gesetzgebung fehlt**, die einen **angemessenen Schutz gewährleistet** und keiner der unter Art. 6 Abs. 2 DSG aufgeführter „Garantien“ zum Tragen kommt.
- Zu beachten ist, dass Art. 6 DSG **kumulativ** zu den übrigen Datenbearbeitungsgrundsätzen gilt!

Bekanntgabe

- Eine Bekanntgabe liegt nicht nur dann vor, wenn die Daten aktiv übermittelt werden, sondern auch, wenn der **Online-Zugriff** auf Daten gewährt wird.
- Eine Bekanntgabe setzt aber voraus, dass die Daten **einem Dritten zugänglich gemacht werden** – der Personenkreis, der die Daten bearbeitet, wird ausgedehnt. Dies gilt auch innerhalb des Unternehmens!
- Die Gewährung des Online-Zugriffs auf das firmeninterne Netzwerk an den IT-Spezialisten des ausländischen Hauptsitzes unterliegt daher Art. 6 DSG.
- Das Outsourcing der Datenbearbeitung an ein ausländisches Unternehmen fällt ebenfalls unter Art. 6 DSG.

Keine Bekanntgabe

- Keine Bekanntgabe im Sinn dieser Bestimmung liegt vor, wenn
  - die Daten **der betroffenen Person selbst** mitgeteilt werden
  - ein Mitarbeiter auf seiner Auslandsreise via Internet auf sein **eigenes E-Mail-Postfach** zugreift
  - ein Mitarbeiter auf seiner Auslandsreise **Daten auf seinem Notebook mitführt** und diese nicht Dritten zugänglich macht.
- Werden Personendaten im **Internet** zwecks Information der Öffentlichkeit allgemein zugänglich gemacht, dann gilt dies nicht als Datenübermittlung ins Ausland (Art. 5 VDSG).

Angemessener Datenschutz

- Der EDÖB führt eine Liste der Staaten, die in Bezug auf das schweizerische Recht einen angemessenen Datenschutz gewährleisten (Art. 7 VDSG). Zu finden ist diese Liste unter: **http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de**
- Zu beachten ist, dass gemäss dieser Liste in vielen EU-Staaten der angemessene Schutz **nur für den Schutz der Daten von natürlichen Personen** gegeben ist und daher bei einer (gleichzeitigen) Übermittlung von Daten von juristischen Personen dennoch zusätzliche Garantien erforderlich wären („Datenübermittlung ins Ausland kurz erklärt“, Erläuterungen des EDÖB).

Garantien

(Art. 6 Abs. 2 DSG)

Bei fehlender Gesetzgebung Bekanntgabe ins Ausland nur, wenn

- hinreichende Garantien, insbesondere durch **Vertrag** vorliegen
- die Einwilligung der betroffenen Person im Einzelfall vorliegt
- die Datenübermittlung im Zusammenhang mit Vertragsabwicklung erfolgt
- überwiegendes öffentliches Interesse vorliegt oder die Datenübermittlung zur Durchsetzung von rechtlichen Ansprüchen vor Gericht erforderlich ist
- die Bekanntgabe Leben und körperliche Integrität schützt
- die Daten allgemein zugänglich gemacht wurden und kein entsprechendes Verbot vorliegt
- innerhalb derselben juristischen Person oder Gesellschaft mit angemessenen Datenschutzregeln (**Konzernregeln**, **Binding Corporate Rules**).

Informationspflichten

- Verträge gemäss Art. 6 Abs. 2 lit. a DSG und Konzernregeln nach Art. 6 Abs. 2 lit. g DSG müssen dem EDÖB **vor der Übermittlung** als Kopie vorgelegt werden.
- Der EDÖB prüft die Dokumente und teilt das Ergebnis innerhalb von 30 Tagen mit.
- Erfolgt anschliessend eine Datenübermittlung auf der Basis der selben Dokumente, dann gilt die Informationspflicht als erfüllt, sofern sich die Rahmenbedingungen nicht geändert haben (z.B. Empfängerkreise).

Musterverträge

- Der EDÖB anerkennt den Standardvertrag „**Swiss Transborder Data Flow Agreement**“ oder die **EU-Standardvertragsklauseln** für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern vom 5. Februar 2010 als hinreichende vertragliche Datenschutzgarantien im Sinn von Art. 6 Abs. 2 lit. a DSG. Über deren Verwendung muss der EDÖB nur informiert werden.
- ACHTUNG! Das „Swiss Transborder Data Flow Agreement“ regelt das **Outsourcing** von Daten.
- Liegt kein reines Outsourcing vor (d.h. die Daten werden durch den Empfänger auch **für eigene Zwecke** bearbeitet), dann handelt es sich wiederum um einen individuellen Vertrag, der dem EDÖB vorgelegt werden muss

Datenübermittlung in die USA

- Werden Daten in die USA übermittelt (beispielsweise elektronische Kundendaten an ein Rechencenter in den USA), dann werden Daten in einen Staat übermittelt, in welchem **kein angemessenes Schutzniveau** herrscht.
- Es muss daher entweder eine der Garantien gemäss Art. 6 Abs. 2 DSG vorliegen (z.B. Vertrag oder Einwilligung) oder es muss sichergestellt werden, dass der Empfänger der Daten sich zur Einhaltung der im U.S.-Swiss Safe Harbor Framework gestellten Bedingungen verpflichtet hat (Zertifizierung).

U.S.-Swiss Safe Harbor Agreement

- Es handelt sich um ein Abkommen mit den USA, wonach ein US-Unternehmen sich zur Einhaltung bestimmter Datenschutz-grundsätze öffentlich verpflichten kann.
- In diesem Fall entfallen Meldepflichten und es muss kein zusätzlicher Vertrag erstellt werden (**U.S.-Swiss Safe Harbor Framework**; gültig seit Februar 2009; abrufbar unter dem folgenden Link: http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de)

Cloud Computing

- Es handelt sich (aus rechtlicher Sicht) einen **Outsourcingvertrag**, welcher die folgenden Merkmale aufweist:
  - Die Leistungen weisen einen hohen Grad an Standardisierung auf.
  - Der Kunde hat keine Kontrolle über den aktuellen Standort seiner Daten.
  - Daten werden in der Regel (auch) im Ausland bearbeitet.
  - Die Menge der geforderten Leistung kann variieren (Skalierbarkeit).
  - Es besteht eine grosse Abhängigkeit vom Netz.

Zulässigkeit des Outsourcings

- Ein Outsourcing liegt vor, wenn ein Unternehmen ein anderes Unternehmen (Dienstleister) beauftragt, eine Dienstleistung **selbständig und dauernd** zu erbringen (sinngemäss: FINMA-Rundschreiben 2008 / 07 Outsourcing Banken).
- Die Auslagerung von Geschäftsbereichen und –aufgaben an Dritte ist heute gelebte wirtschaftliche Realität und ist sowohl im privatrechtlichen als auch im öffentlich-rechtlichen Bereich **grundsätzlich erlaubt**, sofern dabei die **gesetzlichen Vorgaben** eingehalten werden.
- Bereits in der Planungsphase sollten daher im Rahmen einer Risikoanalyse nicht nur die technischen und organisatorischen sondern auch die **rechtlichen Grundlagen** erhoben und berücksichtigt werden!

Outsourcing der Datenbearbeitung

(Art 10a DSG)

- Das DSG gilt für die Bearbeitung von Daten von **natürlichen und von juristischen Personen**, daher werden in der Regel die datenschutzrechtlichen Vorgaben zu beachten sein.
- Gemäss Art. 10a DSG kann die Datenbearbeitung an einen Leistungserbringer übertragen werden, wenn
  - die Daten nur so bearbeitet werden, wie der Auftraggeber es selbst tun dürfte (**Zweckbindung**),
  - keine gesetzliche oder vertragliche **Geheimhaltungspflicht** es verbietet und
  - der Auftraggeber sich vergewissert, dass die **Datensicherheit** gewährleistet ist.

Übermittlung ins Ausland

(Art. 6 DSG)

- Befinden sich Rechenzentren des Cloud-Anbieters (oder seiner Subunternehmer) im Ausland, dann muss **zusätzlich** Art. 6 DSG beachtet werden.
- Die Übermittlung ins Ausland ist nur zulässig, wenn im Empfängerstaat eine (Datenschutz)Gesetzgebung herrscht, welche einen **angemessenen Schutz** gewährleistet.
- Ist dies nicht der Fall, dann muss der angemessene Schutz durch zusätzliche Garantien (Art. 6 Abs. 2 DSG) hergestellt werden – dazu zählt insbesondere der Abschluss von Verträgen mit dem Datenempfänger oder die Einwilligung der betroffenen Personen.

Datenübermittlung in Drittstaat

- In der Praxis werden meist **Verträge mit den Datenempfängern** vereinbart, welche einen angemessenen Schutz im Ausland gewährleisten (Art. 6 Abs. 2 lit. a DSG).
- Erfolgt die Datenübermittlung an eine Konzerngesellschaft, dann können auch **verbindliche Konzernregelungen** geschaffen werden (Art. 6 Abs. 2 lit. g DSG; Binding Corporate Rules) .
- Sowohl der Vertrag als auch die Konzernregelungen müssen dem EDÖB vorgelegt werden.
- Eine Ausnahme besteht, wenn die **EU-Standardvertragsklauseln** oder der **Mustervertrag** des EDÖB für das Outsourcing ins Ausland verwendet werden. In diesen Fällen muss der EDÖB nur über deren Verwendung informiert werden.

Geheimhaltungsvorschriften

(Art. 162 StGB)

- Die Verletzung von Geschäfts- und Fabrikationsgeheimnissen ist **strafbar** (Art. 162 StGB).
  - Bestraft wird, wer ein Geschäfts- oder Fabrikationsgeheimnis, das er aufgrund einer gesetzlichen oder vertraglichen Pflicht bewahren soll, verrät oder für sich oder andere ausnutzt.
- Verträge mit Lieferanten oder Kunden verbieten häufig die Weitergabe von Geschäfts- oder Fabrikationsgeheimnissen an Dritte – dies muss durch ausreichende Sicherheitsmassnahmen gewährleistet werden.

Wirtschaftlicher Nachrichtendienst

(Art. 273 Abs. 2 StGB)

Bestraft wird,

- wer ein Fabrikations- oder Geschäftsgeheimnis einer fremden amtlichen Stelle oder einer ausländischen Organisation **oder privaten Unternehmung** oder ihren Agenten **zugänglich macht**.
- Die Strafe beträgt Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

Voraussetzungen für die Strafbarkeit

- Verboten ist somit **jedes Verhalten**, welches es einem ausländischen Adressaten ermöglicht, in schweizerische Geschäftsgeheimnisse Einblick zu nehmen.
- Dass es tatsächlich zu einer Schädigung kommt, ist für die Erfüllung des Tatbestandes irrelevant (**abstraktes Gefährdungsdelikt**).
- Jedes in der Schweiz ansässige in- und ausländische Unternehmen zählt als „schweizerisches Unternehmen“ – jede Preisgabe eines Geschäfts- oder Fabrikationsgeheimnisses wird als Gefährdung der Schweizerischen Volkswirtschaft gesehen.

Zu beachten

- Um bei einem Outsourcing der Datenbearbeitung ins Ausland nicht mit Art. 273 StGB in Konflikt zu kommen, sind die folgenden Punkte zu beachten:
  - Für gewisse Branchen wie z.B. für Banken besteht ein erhöhtes Risiko (Bankgeheimnis).
  - Die Zustimmung des Geheimnisträgers schützt in der Regel vor Strafbarkeit – Zustimmung wenn möglich in AGB einholen!
  - Es ist grosser Wert auf die Ausarbeitung der Outsourcingverträge zu legen – Zugriffsberechtigungen, Kontrollrechte und deren Durchführung sind essentielle Faktoren!

Weitere gesetzliche Anforderungen

- Da die Cloud-Dienstleistungen in der Regel **Standard-Leistungen** beinhalten, muss das Unternehmen vor dem Vertragsabschluss überprüfen, ob diese den gesetzlichen Anforderungen entsprechen.
- Es sind beispielsweise die **handels- und steuerrechtlichen Vorgaben** an die elektronische Aufbewahrung und Archivierung von Geschäftsdokumenten zu beachten.
- Beispiele:
  - Integrität der Dokumente (Art. 9 GeBüV),
  - Dauer der Aufbewahrung (in der Regel 10 Jahre ab Ende des Geschäftsjahres)
  - Zulässigkeit der Aufbewahrung im Ausland (Art. 10 Abs. 4 ElDI-V)
  - Bei einem Dienstleister im Ausland: Muss MwSt abgeliefert werden?

Planung und Umsetzung

- Die genannten Bestimmungen müssen bereits in der Planungs- und Evaluationsphase berücksichtigt werden.
- In einem **ersten Schritt** sollte geklärt werden, ob eine Auslagerung generell und speziell ins Ausland allenfalls durch **Geheimhaltungspflichten** verboten oder an besondere Bedingungen gebunden ist (Beispiel: Banken, Ausgleichskassen, etc.).
- Anschliessend sollte ein **Anforderungskatalog** erstellt werden, in dem die Muss- und Kann-Anforderungen festgehalten werden.
- Zu beachten ist, dass gewisse Risiken nicht vertraglich eliminiert werden können – untersteht der Cloud-Anbieter einer fremden Rechtsordnung, dann muss unter Umständen einer ausländischen Behörde der Zugriff auf die Daten gewährt werden.

Datensicherheit

(Art. 7 DSG i.V.m. Art.8-11 sowie 21 und 22 VDSG)

- Der Auftraggeber muss **angemessene technische und organisatorische Massnahmen** ergreifen, damit die Daten gegen **unbefugtes Bearbeiten** geschützt werden.
- Im Rahmen der Auslagerung in die Cloud muss der Auftraggeber daher insbesondere
  - den Anbieter sorgfältig auswählen (Einholen von Referenzen)
  - sich vor Vertragsabschluss vergewissern, dass die Sicherheitsmassnahmen des Cloud-Anbieters dem Schutzbedarf der auszulagernden Daten entspricht
  - es darf nicht zu einer Vermischung der Daten unterschiedlicher Anwender kommen
  - allenfalls zusätzliche Massnahmen vereinbaren (Service Level Agreements)

Kontrollrechte

- Gemäss Art. 10a Abs. 2 DSG muss sich der Auftraggeber **vergewissern**, dass die **Datensicherheit** eingehalten wird.
- Es genügt nicht, wenn der Auftraggeber die Datensicherheit nur bei Vertragserstellung beachtet – er bleibt trotz Auslagerung für die Datensicherheit verantwortlich.
- Je nach **Risikobeurteilung** sind unterschiedliche Massnahmen zu treffen:
  - Vereinbarung eines Kontrollrechts für sich und / oder für von ihm beauftragte Dritte
  - Zertifizierung des Anbieters und Einsicht in Auditberichte
  - Informationspflicht bei wichtigen Vorkommnissen
- Sind diese Massnahmen nicht umsetzbar, dann muss bei einem hohen Risiko auf das Auslagern in die Cloud verzichtet werden.

Weitere wichtige Vertragspunkte I

- Die genaue Definition der durch den Vertragspartner geschuldeten Leistung (inklusive Betrieb) ist eine wesentliche Massnahme zur Reduktion der eigenen Risiken.
- Es sollte schriftlich festgelegt werden, **welche AGB** in welcher Version Vertragsbestandteile bilden und alle **abweichenden Punkte** sind im Vertrag festzuhalten!
- Der Anbieter muss verpflichtet werden, die Daten **nur für die vereinbarten Zwecke** zu verwenden.
- Sämtliche **Subunternehmer** müssen genannt werden – der Beizug weiterer Subunternehmer sollte an eine vorgängige Zustimmung des Auftraggebers gebunden werden.
- Es muss vereinbart werden, in welchen **Ländern** die Daten bearbeitet werden.

Weitere wichtige Vertragspunkte II

- Die **Verantwortungen** müssen geregelt sein (Mitwirkungspflichten des Auftraggebers, Systemgrenzen).
- Aus der **Vereinbarung** muss klar hervorgehen, **welche Leistungen in welcher Menge und Qualität** bezogen werden.
- Die Qualität der Dienstleistungen sollte in **Service Level Agreements** nachvollziehbar und überprüfbar vereinbart werden (Konventionalstrafen).
- Die **Haftung** des Anbieters bei Vertragsverletzungen muss den unternehmerischen Risiken des Auftraggebers entsprechen.
- Das **Auskunftsrecht** (Art. 8 DSG) der betroffenen Person und das Recht auf **Löschung** und **Berichtigung** der Daten (Art. 5 DSG) müssen jederzeit gewährleistet sein.

Vertragsauflösung und Folgen

- Um eine möglichst grosse **Unabhängigkeit** vom Anbieter zu bewahren, sollte vertraglich sichergestellt werden, dass ein Wechsel zu einem anderen Anbieter jederzeit möglich ist.
- Die **Kündigungsfristen** müssen den eigenen unternehmerischen Bedürfnissen entsprechen.
- Der Anbieter muss verpflichtet werden, bei Vertragsauflösung die erforderliche **Unterstützung** für die Migration der Daten und Dokumente auf die Systeme des neuen Vertragspartners zu leisten – die Kosten dieser Unterstützung sollten vertraglich vereinbart werden.
- Die Verwendung standardisierter Technologien und Schnittstellen sollte vereinbart werden (**Portabilität**).

Zusammenfassung

- Cloud Computing stellt aus rechtlicher Sicht nicht vollkommen neue Anforderungen.
- Im Vergleich zu einem „normalen“ Outsourcingvertrag stellen insbesondere die **mangelnde Kontrolle über den physischen Standort der Daten**, die mögliche **Vermischung mit den Daten anderer Nutzer**, die **Portabilität** sowie der allfällige **Zugriff ausländischer Behörden** erhöhte Risiken dar.
- Gut durchdachte und sorgfältig verhandelte Verträge, die sorgfältige Auswahl des Anbieters , die Vereinbarung von Kontrollrechten und Informationspflichten sowie die Regelung der Folgen der Vertragsauflösung sind zentrale Elemente der Risikoreduktion!
- Auftraggeber müssen sich bewusst sein, dass die **Verantwortung** für die Einhaltung der gesetzlichen Vorgaben primär bei ihnen liegt und nicht beim Cloud-Anbieter!

Nützliche Links

- **Erläuterungen des EDÖB zu Cloud Computing**
  http://www.edoeb.admin.ch/datenschutz/00626/00876/index.html?lang=de
- **Erläuterungen des EDÖB zur Datenübermittlung ins Ausland**
  http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de
- **Erläuterungen des EDÖB zu Outsourcing (inklusive Mustervertrag für das Outsourcing ins Ausland)**
  http://www.edoeb.admin.ch/datenschutz/00626/00753/00969/index.html?lang=de
- **Merkblatt des Datenschutzbeauftragten ZH zu Cloud Computing**
  https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/organisation_und_technik.html
- **Cloud-Computing-Strategie der Schweizer Behörden 2012-2020**
  http://www.egovernment.ch/de/umsetzung/cloud-strategie.php