TAGUNG FÜR INFORMATIK UND RECHT

Nutzung von Cloud Lösungen – Rechtliche Rahmenbedingungen für Behörden

12. November 2018

Dr. Ursula Widmer, Rechtsanwältin
Dr. Widmer & Partner, Rechtsanwälte, Bern
ursula.widmer@widmer.ch
+41 79 300 32 38 / +41 31 351 66 33

Nutzung von Cloud Lösungen: Rechtliche Rahmenbedingungen für Behörden

Inhaltsübersicht

- Cloud Services für Behörden
- Gesetzliche Rahmenbedingungen - Überblick
- Datenschutz
  - Personendaten / Aufhebung des Personenbezugs
  - Auftragsbearbeitung
  - Datenweitergabe ins Ausland
- Geheimhaltungspflichten
- Verfahrensmässige Pflichten

Trends bei der Beschaffung von Cloud Services

Bundesbehörden, kantonale Behörden, Gemeinden, Spitäler usw. wollen Services aus der Cloud beschaffen:

- Cloud Computing Plattformen wie Microsoft Azure, Google App Engine oder Elastic Compute Cloud von Amazon für den Betrieb eigener Applikationen und/oder das Storage von grossen Datenmengen
- Office Produkte
- HR- und ERP-Applikationen
- Netzwerkmonitoring, Security und Data Center Services
- Marketing (z.B. Newsletter)
- usw.

Cloud Computing Strategie der Schweizer Behörden 2012-2020

Empfehlungen, keine bindende Vorgabe

- **Strategischer Grundsatz G2 – Cloud first**
  „Bei Neuentwicklungen und Anschaffungen wird systematisch geprüft, ob geeignete Cloud-Angebote vorhanden sind. Eine Cloud-Lösung wird gewählt, wenn sie die Gesamtheit der Anforderungen insbesondere an Funktionalität, Wirtschaftlichkeit und Sicherheit über alles betrachtet am besten abdeckt. …… “

- **Strategischer Grundsatz G9 - Sicherheit**
  „Aspekten der Sicherheit, des Datenschutzes und des Risikomanagements wird bei der Evaluation und beim Einsatz von Cloud-Computing-Lösungen gebührend Rechnung getragen.“

Gesetzliche Rahmenbedingungen Bund zur Nutzung von Cloud Services

- Datenschutzgesetz (in Revision)
- Schengen-Datenschutzgesetz (für den Bereich Polizei, Strafverfolgung und Strafvollstreckung)
- Bundesinformatikverordnung und Ausführungsbestimmungen
  - Weisungen Bundesrat über IKT-Sicherheit
  - Sicherheitsvorgaben des ISB, insb. IKT Grundschutz
- Bereichsspezifische Regelungen
  - Personalrecht, insb. VO über den Schutz von Personendaten des Bundespersonals
  - Gesundheitsrecht, z.B. Humanforschungsgesetz

Gesetzliche Rahmenbedingungen Bund zur Nutzung von Cloud Services

- Geheimhaltungspflichten
  - Berufliche Schweigepflicht (Art. 35 DSG)
  - Amtsgeheimnis (Art. 320 StGB)
  - Berufsgeheimnis (Art. 321 StGB)
  - Schweigepflicht im Sozialversicherungsrecht (Art. 33 ATSG)
  - Opferhilfegesetz (Art. 11 OHG)
  - etc.

Gesetzliche Rahmenbedingungen Kantone zur Nutzung von Cloud Services

- Kt. Datenschutzgesetzgebung
- Kt. Gesetzgebung betreffend Informatik und Informationssicherheit
- Sektorspezifische Bestimmungen, z.B.
  - Personalrecht
  - Gesundheitsrecht
- Strafgesetzbuch
  - Verletzung des Berufsgeheimnisses (Art. 321)
  - Verletzung des Amtsgeheimnisses (Art. 320)

Gesetzliche Rahmenbedingungen Kantone zur Nutzung von Cloud Services

- Kt. Allgemeine Geschäftsbedingungen
  - **Kanton BE:** AGB über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen (AGB ISDS) vom 24.3.2015
  - **Kanton ZH:** AGB bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen vom 24.6.2015
  - **Kanton SO:** AGB über die Informationssicherheit und den Datenschutz bei der Erbringung von Informatikdienstleistungen (AGB ISDS) vom 28.11.2016

Zulässigkeit von IT-Auslagerungen?

Nutzung von Cloud Services kann ausgeschlossen sein, wegen z.B.

- Verbot von IT-Auslagerungen (mit Möglichkeit zu Ausnahmebewilligungen)

  Kanton Thurgau: Reglement Regierungsrat über den Einsatz der Informatik

  - Grundsatz: Verwendung fremder Hard- und Software untersagt
  - Ausnahmen möglich: braucht aber Einverständnis Amt für Informatik

- Gesetzliche Festlegung des technischen Bertreibers von Systemen

  Bund: VO über den Schutz von Personendaten des Bundespersonals

  - BIT als technischer Betreiber der wesentlichen zentralen Systeme zur Verarbeitung der Daten des Bundespersonals

Datenschutz - Begriffe die Sie kennen sollten

- **Personendaten** - Art. 3 a DSG

  *«Alle Angaben, welche sich auf eine **bestimmte oder bestimmbare** natürliche oder juristische Person beziehen.»*

- **Besonders schützenswerte Personendaten** - Art. 3 c DSG

  «Personendaten, über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre und die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe sowie über administrative oder strafrechtliche Verfolgungen und Sanktionen.»

- **Persönlichkeitsprofile** - Art. 3 d DSG (**Profiling** - Art. 4 f DSG in Revision)

  *«Zusammenstellungen von Daten, die eine **Beurteilung wesentlicher Aspekte der Persönlichkeit** einer **natürlichen Personen** erlauben.»*

- **Bearbeiten** - Art. 3 e DSG

  «Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.»

Aufhebung des Personenbezugs

- **Verschlüsselung**

  *«Anwendung **kryptographischer Verfahren zur Gewährleistung der Vertraulichkeit und der Integrität der Daten** und i.w.S. der Authentifizierung des Absenders von Daten, damit kein Unberechtigter die Daten einsehen oder manipulieren kann.» - Gabler Wirtschaftslexikon*

- **Pseudonymisierung**

  *«Die **Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.» - Art. 4 Nr. 5 EU-DSGVO*

- **Anonymisierung**

  «Zur Anonymisierung [von Personendaten] ***müssen alle Angaben, die in ihrer Kombination die Wiederherstellung des Bezugs zu einer Person ohne unverhältnismässigen Aufwand erlauben, irreversibel unkenntlich gemacht** oder gelöscht werden.» - Art. 25 Abs. 1 Humanforschungsverordnung (HFV)*

➡ **Verschlüsselte und pseudonymisierte Daten gelten (gegenüber Dritten ohne Zugriffsmöglichkeit auf den Schlüssel) nicht als Personendaten.**

➡ **Anonymisierte Daten haben keinen Personenbezug mehr und sind somit keine Personendaten.**

Auftragsdatenbearbeitung Gesetzliche Grundlagen Bund

Datenbearbeitung durch Dritte (DSG Art. 10a*)*

[1] Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:

a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

[2] Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.

[3] ……

Bearbeitung durch Auftragsbearbeiter (SDSG Art. 10)

[1] Die Bearbeitung von Personendaten kann einem Auftragsbearbeiter übertragen werden, wenn er die Voraussetzungen nach Art. 10a DSG erfüllt.

[2] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Genehmigung des Bundesorgans einem Dritten übertragen.

Auftragsdatenbearbeitung Gesetzliche Grundlagen Bund (Entwurf DSG Sept. 2017)

Bearbeitung durch Auftragsbearbeiter (E-DSG Art. 8) *[EU: Auftragsdatenverarbeitung]*

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

[4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Auftragsdatenverarbeitung
Gesetzliche Grundlagen Kantone

Bearbeiten im Auftrag (KDSG BE Art. 16)

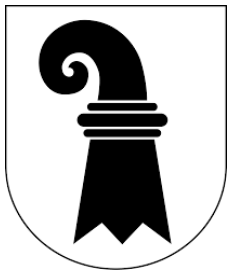
[1] Wer Personendaten im Auftrag einer Behörde bearbeitet, untersteht dem Gesetz wie der Auftraggeber. Zur Bekanntgabe von Personendaten an Dritte bedarf er der ausdrücklichen Zustimmung des Auftraggebers.

Bearbeiten im Auftrag (IDG BS § 7)

[1] Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn:

a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und
b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte.

[2] Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.



Auftragsdatenbearbeitung - Datenschutz

Grundsätze

- Auftragsdatenbearbeitung ist für Personendaten zulässig
- Einwilligung der betroffenen Personen nicht erforderlich
- Auftraggeber bleibt für die Einhaltung des Datenschutzes verantwortlich
  - Clouddienstleister darf Daten nur so bearbeiten, wie es der Auftraggeber selbst auch darf
  - Auftraggeber muss Einhaltung der Datensicherheit durch Clouddienstleister sicherstellen
- Keine Verletzung von Geheimhaltungsvorschriften

➡ **Vertrag zwischen Auftraggeber und Clouddienstleister zwingend**

Auftragsdatenbearbeitung – Vertrag

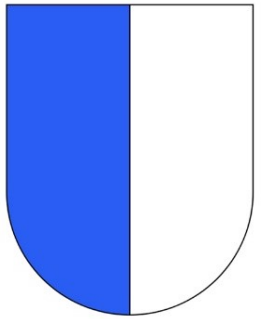
Wesentliche Vertragspunkte

- Gesetzliche Vorgaben in einzelnen Kantonen, z.B.

  Kanton Luzern Informatikgesetz: § 13 Zulässigkeit von IT-Auslagerungen

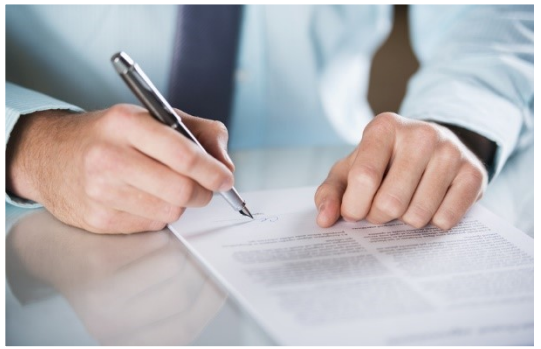
  [1] .....

  [2] Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: .
  a. Inhalt der Dienstleistung,
  b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten,
  c. Verantwortlichkeiten,
  d. verwendete Techniken, einschliesslich Entwicklung und Wartung,
  e. Zugriffs- und Zutrittsrechte,
  f. Sicherheits- und Datenlöschkonzept,
  g. Standorte der Hardware und der Datenbearbeitung,
  h. Kontrollrechte,
  i. Beizug von Dritten,
  j. Archivierung,
  k. Rückführung und Löschung der Daten im Fall der Vertragsauflösung.



- Privatim: Merkblatt Cloud Computing im Schulbereich

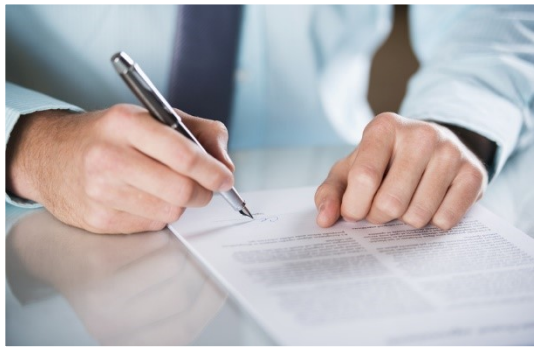
Auftragsdatenbearbeitung – Vertrag



Wesentliche Vertragspunkte

- Sicherstellung der Datenschutzgrundsätze
  - Gegenstand der Datenbearbeitung
    - Definition der Kategorien von Daten, welche im Auftrag bearbeitet werden
  - Umfang der Datenbearbeitung durch Clouddienstleister
    - Bearbeitung nur soweit für die Erbringung der Clouddienste erforderlich
  - Zweckbindung der Datenbearbeitung durch den Clouddienstleister
    - Ausschluss der Bearbeitung der Daten für andere Zwecke als im Vertrag vereinbart
  - Abgrenzung der Verantwortlichkeit zwischen Auftraggeber und Clouddienstleister
  - Verfügungsmacht des Auftraggebers über die Daten
    - Zugriff auf die Daten, Möglichkeit zur Extrahierung während Vertragslaufzeit und bei Vertragsende

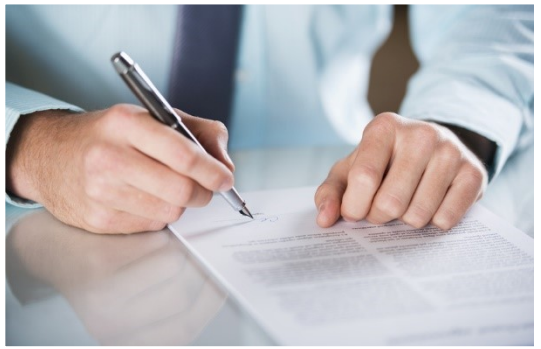
Auftragsdatenbearbeitung – Vertrag



Wesentliche Vertragspunkte (Forts.)

- Festlegung der Zugriffsberechtigungen des Clouddienstleisters bzw. von dessen Mitarbeitenden auf die Daten
- Voraussetzungen für eine allfällige Bekanntgabe der Daten durch den Clouddienstleister
  - nur auf Weisung des Auftraggebers oder wenn explizit vereinbart (z.B. Subunternehmer) oder gesetzlich vorgeschrieben
- Vorgehen im Zusammenhang mit der Wahrnehmung der Rechte durch die betroffenen Personen (Auskunft, Berichtigung, Löschung, Sperrung)
  - Pflicht des Clouddienstleisters zur Berichtigung, Löschung, Sperrung von Daten, sofern der Kunde dies nicht selber kann
- Geheimhaltungsverpflichtungen
  - Verpflichtung der Mitarbeitenden des Clouddienstleisters zur Geheimhaltung betreffend Kundendaten

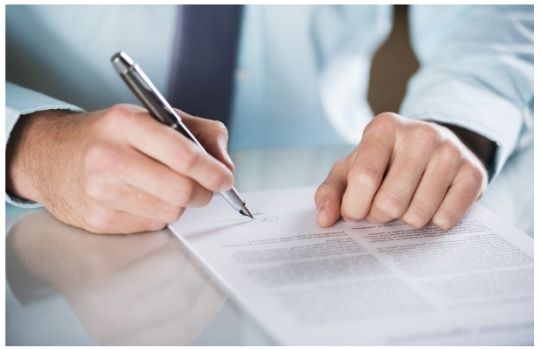
Auftragsdatenbearbeitung – Vertrag



Wesentliche Vertragspunkte (Forts.)

- Folgen der Vertragsauflösung
  - Möglichkeit des Auftraggebers zur Extrahierung seiner Daten
  - Löschung der Daten durch Clouddienstleister
- Datensicherheit
  - Pflicht zur Vorkehrung von organisatorische und technische Massnahmen zur Wahrung des Datenschutzes und der Datensicherheit
  - Anforderungen betreffend Sicherheitszertifizierung(en)

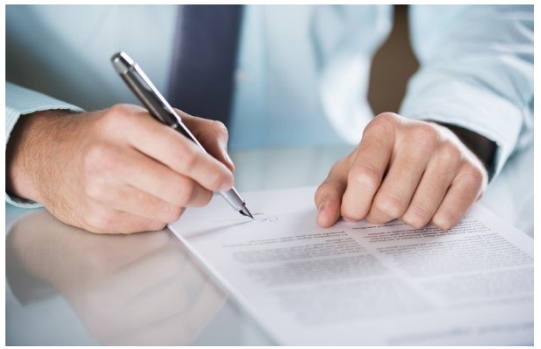
Auftragsdatenbearbeitung – Vertrag



Wesentliche Vertragspunkte (Forts.)

- Kontrolle
  - Weisungsrecht des Auftraggebers mit Bezug auf die Bearbeitung der Personendaten durch den Clouddienstleister
    - z.B. bezüglich der Bekanntgabe von Daten an Dritte, Löschung von Daten falls von Betroffenen verlangt
  - Ort(e) der Datenbearbeitung, das heisst Standort(e) der Server
  - Informationspflicht des Clouddienstleisters bei Verletzungen des Datenschutzes (Data Breaches)
  - Regelung des Beizugs und Wechsels von Subunternehmern
    - Gleiche vertragliche Pflichten wie für den Clouddienstleister

Auftragsdatenbearbeitung – Vertrag

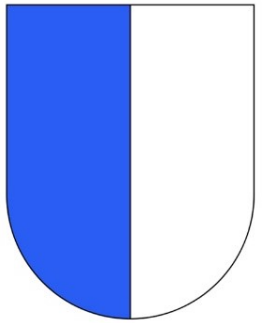


Wesentliche Vertragspunkte (Forts.)

- Verantwortung des Clouddienstleisters für Subunternehmer gegenüber Auftraggeber
- Bekanntgabe der Subunternehmer bei Vertragsabschluss des Vertrages
- Vorgängige Bekanntgabe neuer Subunternehmer, Recht zur ausserordentlichen Vertragsbeendigung des Auftraggebers bei Nichteinverständnis

- Pflicht zur Vornahme von Sicherheitsaudits durch Auftragsbearbeiter und Vorlage von der Berichte / Möglichkeit zur Vornahme von Audits durch die auslagernde Behörde bzw. deren beauftragte Fachspezialisten
- Sicherstellung des Zugangs / Zugriffs für Aufsichtsbehörden (z.B. Kt. LU, BE, ZH)
- Anwendbarkeit von Schweizer Recht und Gerichtsstand in der Schweiz
  - Mit Bezug auf die Bestimmungen zur Datenverarbeitung gilt Schweizer Recht und Gerichtsstand Zürich

Auftragsdatenbearbeitung – Vertrag

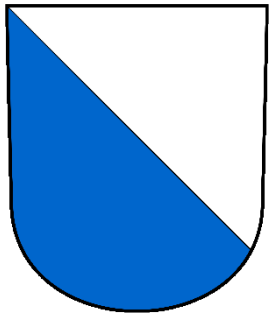


Kantonales Recht

- Grundsätzlich gelten die Anforderungen gemäss dem DSG auch für die dem kantonalen Recht unterstehenden Behörden
- Einzelne Kantone kennen Sonderregelungen

  Beispiel: Informatikgesetz Kanton Luzern (§ 15 Abs. 2):
  - Auftraggeber und kantonale Datenschutzbehörde und kantonale Finanzkontrolle müssen Zutritt zu den Räumen und Anlagen des Clouddienstleisters sowie Zugriffsrechte auf Daten haben

Auftragsdatenbearbeitung – Vertrag

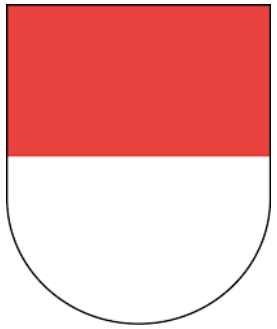


Kanton Zürich: AGB Auslagerung Informatik

- Gelten für alle öffentlichen Organen, die dem kantonalen Datenschutzgesetz unterstehen
- Müssen als Bestandteil des Vertrages mit dem Auftragsdatenbearbeiter vereinbart werden
- Beinhalten zusätzliche Anforderungen insb.
  - Informationssicherheit
    - Pflicht zu Sicherheitsmanagement/-organisation/-konzept;
    - Geltung ISO/IEC 27000-Serie oder BSI Grundschutzstandard 100-1 bis 100-4
    - Trennung von Informationsbeständen;
    - Dokumentationspflicht Anbieter: Methoden / Prozesse zur Wahrung der Sicherheit
  - Speicherung und Archivierung von Daten nur mit schriftlicher Genehmigung des öffentlichen Organs ausserhalb der Schweiz;
  - Zusatzbedingungen Cloud Computing
    - Informationspflicht über eingesetzte Technologie und deren Weiterentwicklung
    - Information über sämtliche möglichen Datenverarbeitungsorte
    - Umfassende Verschlüsselung aller Daten in der Cloud; Schlüsselverwaltung beim öffentlichen Organ

Auftragsdatenbearbeitung – Vertrag

Kantone Bern und Solothurn: AGB ISDS



- Gelten für die Kantonsverwaltung sowie für weitere Stellen, für welche das kantonale Datenschutzgesetz gilt
- Müssen als Bestandteil des Vertrages mit dem Clouddienstleister vereinbart werden
- Beinhalten zusätzliche Anforderungen
  - Ähnlich AGB Kt. ZH, aber nicht gleich (z.B. keine spezifischen Bedingungen betreffend Cloud Computing)

Auftragsdatenbearbeitung - Datensicherheit

Datensicherheit (DSG Bund Art. 7)

[1] Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

[2] Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Technische und organisatorische Massnahmen - Grundsatz (DSV BE Art. 4)

[1] Die verantwortliche Behörde, die Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt mit technischen und organisatorischen Massnahmen für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten (Art. 17 KDSG) ….

Informationssicherheit (IDG BS § 8)

[1] Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.

[2] Die Massnahmen richten sich nach den folgenden Schutzzielen:
a) Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (Vertraulichkeit); ….

Auftragsdatenbearbeitung - Datensicherheit

VO zum DSG Bund Art. 8: Allgemeine Massnahmen

[1] Wer als Privatperson Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, um einen angemessenen Datenschutz zu gewährleisten. Insbesondere schützt er die Systeme gegen folgende Risiken:

a. unbefugte oder zufällige Vernichtung;
b. zufälligen Verlust;
c. technische Fehler;
d. Fälschung, Diebstahl oder widerrechtliche Verwendung;
e. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

[2] Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere tragen sie folgenden Kriterien Rechnung:

……

Analog: Kanton Bern (Art. 4 DSV) und Kanton Basel-Stadt (§ 8 IDG)

Auftragsdatenbearbeitung – Datensicherheit

VO zum DSG Bund Art. 9: Besondere Massnahmen

[1] Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:

a. Zugangskontrolle …
b. Personendatenträgerkontrolle …
c. Transportkontrolle …
d. Bekanntgabekontrolle …
e. Speicherkontrolle …
f. Benutzerkontrolle …
g. Zugriffskontrolle …
h. Eingabekontrolle …

Auftragsdatenbearbeitung – Datensicherheit

Kantonales Recht

- Grundsätzlich gelten die Anforderungen gemäss DSG/VDSG auch für die dem kantonalen Recht unterstehenden öffentlichen Unternehmen und Organisationen
- Einzelne Kantone kennen Sonderregelungen
- Kanton Zürich: AGB Auslagerung Informatik
  - **Information über Methoden und Prozesse:** Auftragnehmer ist betreffend Methoden und Prozesse zur Wahrung der Datensicherheit zu informieren; Recht zur Einsichtnahme in Unterlagen vor Ort und zum Demonstrierenlassen von Prozessen
  - **Cloud Services:** Umfassende Informationspflicht des Clouddienstleisters betreffend Methoden und Technologien; Informationspflicht über sämtlichen möglichen Datenverarbeitungsorte; Transfer und Speicherung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen nur mit «umfassender kryptographischer Sicherung»
- Kantone Bern und Solothurn: AGB ISDS
  - **Information über Methoden und Prozesse:** Auftragnehmer ist betreffend Methoden und Prozesse zur Wahrung der Datensicherheit zu informieren; Recht zur Einsichtnahme in Unterlagen vor Ort und zum Demonstrierenlassen von Prozessen

Datenweitergabe ins Ausland – Gesetzliche Anforderungen

Schweiz (Datenexport)

Datenimporteure

EU, EFTA, Kanada, Argentinien, Uruguay, Israel, Neuseeland, Australien (bedingt)	**USA** Privacy Shield Framework	**Übrige**
angemessener Schutz keine Massnahmen nötig	Privacy Shield Zertifizierung = angemessener Schutz keine Massnahmen nötig	kein angemessener Schutz
	ohne Privacy Shield Zertifizierung: kein angemessener Schutz vertragliche Garantien nötig	vertragliche Garantien nötig

Datenbekanntgabe (Export) ins Ausland

Grenzüberschreitende Bekanntgabe (DSG Art. 6)

[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

[2] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; ……

Bekanntgabe ins Ausland (KDSG BE Art. 14a)

[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

[2] Trotz fehlender Gesetzgebung, die einen angemessenen Schutz gewährleistet, können Personendaten ins Ausland bekannt gegeben werden, wenn

a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten, ……

Datenweitergabe ins Ausland – Gesetzliche Anforderungen

- Keine Datenweitergabe ins Ausland, wenn Persönlichkeit der Betroffenen schwerwiegend gefährdet
- Im Empfängerland Datenschutzgesetzgebung notwendig, die angemessenen Schutz gewährleistet
  - Hilfsmittel (nicht verbindlich): Staatenliste des Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (EDÖB)
- Bei Fehlen eine Gesetzgebung mit angemessenem Schutz, vertragliche Garantien erforderlich
  - Standardvertragsklauseln der EU; von EDÖB anerkannt
  - Mitteilung des Vertragsabschlusses an EDÖB erforderlich
- Sonderfall USA: Zertifizierung gemäss Swiss-US Privacy Shield führt zu angemessenem Datenschutz

Datenweitergabe ins Ausland – erhöhtes Risikopotential

- Kontrolle der Vertragseinhaltung durch den Auftragsdatenbearbeiters im Ausland ist aufwändiger als im Inland
- Durchsetzung der Vertragspflichten des Auftragsdatenbearbeiters im Ausland ist schwieriger als im Inland
- Risiko des Zugriffs auf Daten durch ausländische Behörden nicht kontrollierbar

Fazit

- Bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen gelten zusätzliche Schutzmassnahmen allgemein als notwendig,
  - Anonymisierung (sofern vom Nutzungszweck her möglich)
  - genügend starke Verschlüsselung der Daten bei Transfer und Speicherung mit Schlüsselverwaltung beim Auftraggeber in der Schweiz
  - Nutzung weiterer Sicherheitsfeatures, z.B. Trusted Execution Environment für die Bearbeitung der Daten in der Cloud
- Implementierung der Schutzmassnahmen ist im jeweiligen Projekt zu prüfen

Geheimhaltungspflicht

- Geheimhaltungsvorschriften
  - Amtsgeheimnis Art. 320 StGB
  - Berufsgeheimnisse (Arzt, Notar, Pfarrer etc.) Art. 321 StGB
  - Berufliche Schweigepflicht Art. 35 DSG
    - für besonders schützenswerte Personendaten und Persönlichkeitsprofile
  - Schweigepflicht im Sozialversicherungswesen (AHV/IV, KVG, UVG)
  - Opferhilfegesetz (Art. 11 OHG)
  - etc.

- Offenbarung geheimer Informationen ohne Einwilligung der betroffenen Person (Geheimnisherr) ist strafbar

Geheimhaltungspflicht

- Ausnahmen:
  - Kantonale Bestimmungen zur Datenbearbeitung durch Dritte gelten als Ausnahmeregelungen zum Amtsgeheimnis, Datenweitergabe an Auftragsbearbeiter daher zulässig
  - Offenbarung an Hilfspersonen des Geheimhaltungspflichtigen
    - aber nur, wenn in der Schweiz, da strafrechtlicher Schutz im Ausland nicht durchsetzbar. Öffentlich-rechtliche Spitäler dürfen personenbezogene Daten nicht in ausländische Cloud geben (Ausnahme: Verschlüsselung, Anonymisierung)

Geheimhaltungspflicht

- Anwendung der Ausnahmeregelung auf Anbieter wie Cloud Services Provider in CH unklar
  - Im Sozialversicherungswesen gesetzlich vorgesehen (AHVG Art. 49a, KVG Art. 84, UVG Art. 96)
  - Dem Amtsgeheimnis unterstehende Daten: Amt darf auslagern
  - Dem Berufsgeheimnis und der beruflichen Schweigepflicht unterstehende Daten: umstritten
    - teilweise gesetzlich erlaubt (z.B. Art. 12 Patientenrechtsverordnung Kt. BE)

- Immer notwendig: Vertragliche Verpflichtung des Cloud Service Anbieters, seinerseits die Geheimhaltung zu wahren

Verfahrensmässige Pflichten

Informations-, Prüf- und Bewilligungsverfahren für Cloud Projekte, z.B.

- **Kt. TG:** Bewilligungspflicht für die Nutzung von Hard- und Software, an welcher dem Kanton keine Eigentums- bzw. Nutzungsrechte zustehen.
- **Kt. LU:** Genehmigungspflicht durch den Regierungsrat bei IT-Auslagerungen von übergeordnetem oder strategischem Interesse; ebenso Auslagerungen, welche das Personalinformationssystem betreffen.
- **Kt. ZH, BE und andere:** ev. Vorabkontrolle für Cloud-Projekte gemäss Datenschutzgesetzgebung (z.B. bei besonders schützenswerten Personendaten, grosse Zahl betroffener Personen, besondere technische Risiken)
- **Kt. VS/BE:** Genehmigungspflicht bzw. Meldepflicht gem. kantonalem Datenschutzrecht bei Vereinbarung besonderer vertraglichen Datenschutzgarantien mit dem Clouddienstleister

Herzlichen Dank für Ihre Aufmerksamkeit

Dr. Ursula Widmer

Dr. Widmer & Partner · Rechtsanwälte
Schosshaldenstrasse 32
3000 Bern
Tel.: + 41 31 351 66 33
Mobil: + 41 79 300 32 38
E-Mail: ursula.widmer@widmer.ch
www.widmer.ch

Dr. Ursula Widmer ist Rechtsanwältin in Bern, Lehrbeauftragte für Informatikrecht an der Universität Bern und für Recht der Informationssicherheit an der ETH Zürich. Sie ist ehemaliges Mitglied der vom Bundesrat eingesetzten Expertenkommission «Netzwerkkriminalität», ehemaliges Mitglied der Eidgenössischen Datenschutzkommission, ehemaliges Mitglied des Advisory Board des Information Security Forum (ISF), Past Präsidentin der International Technology Law Association (ITechLaw) und Past Präsidentin der Information Security Society Switzerland (ISSS). Sie ist Präsidentin des Stiftungsrates der Deutschen Stiftung für Recht und Informatik (DSRI), Mitglied der vom Bundesrat eingesetzten Expertenkommission zur «Zukunft der Datenbearbeitung und Datensicherheit» und Mitglied des Institutsrates METAS (Eidgenössisches Institut für Metrologie). Ihre Anwaltskanzlei, Dr. Widmer & Partner, Rechtsanwälte in Bern, ist seit über 30 Jahren spezialisiert auf Fragen im Bereich des Technologierechts, Datenschutzrechts und Datensicherheit.