DR. WIDMER & PARTNER · RECHTSANWÄLTE

Schosshaldenstr. 32
CH - 3000 Bern 31

Telefon +41 - 31 - 351 66 33
Telefax +41 - 31 - 351 66 50

E-mail:
lawyers@widmer.ch
www.widmer.ch

Schweizerische Informatikkonferenz
Speichergasse 6
3000 Bern 7

Bern, den 31. Januar 2018/uw

Gutachten

Klärung und Analyse der rechtlichen Grundlagen für die Integration von «Platform-as-a-Service» und «Software-as-a-Service» in der öffentlichen Verwaltung

für

Schweizerische Informatikkonferenz (SIK)

durch

Dr. Ursula Widmer
Dr. Widmer & Partner, Rechtsanwälte, Bern

Inhaltverzeichnis

1. Einleitung ... 3
1.1 Gegenstand und Adressatenkreis ... 3
1.2 Zweck ... 3
1.3 Anhang: Checkliste ... 4
2. Management Summary ... 4
3. Rechtliche Rahmenbedingungen - Übersicht ... 5
3.1 Kantonale Gesetzgebung ... 5
3.2 Datenschutzgesetz des Bundes ... 6
3.3 Geheimhaltungspflichten ... 6
3.4 Exkurs: EU-DSGVO ... 7
3.4.1 Grundsatz – keine Geltung für Schweizer Behörden ... 7
3.4.2 Ausnahmen bei privatrechtlicher Tätigkeit ... 7
4. Datenschutz ... 8
4.1 Personendaten ... 8
4.2 Besondere Kategorien von Personendaten ... 8
4.3 Entpersonalisierung von Daten (Anonymisierung, Pseudonymisierung, Verschlüsselung) ... 9
4.3.1 Rechtliche Relevanz ... 9
4.3.2 Anonymisierung ... 9
4.3.3 Pseudonymisierung ... 10
4.3.4 Verschlüsselung ... 10
5. Datenbearbeitung durch Dritte (Auftragsdatenbearbeitung) ... 10
5.1 Allgemein – Grundsätzliche Zulässigkeit ... 10
5.2 Bearbeitung wie der Auftraggeber ... 12
5.2.1 Vertragliche Vereinbarung notwendig ... 12
5.2.2 Besondere Vertragsbedingungen ... 13
5.3 Datensicherheit ... 15
5.3.1 Allgemeine Anforderungen ... 15
5.3.2 Besondere Anforderungen ... 16
6. Weitergabe ins Ausland ... 17
6.1 Anforderungen gemäss Datenschutzrecht ... 17
6.2 Erhöhte Risiken ... 19
7. Geheimhaltungsvorschriften ... 20
7.1 Allgemeines Amtsgeheimnis – Art. 320 Strafgesetzbuch ... 20
7.2 Weitere Geheimhaltungspflichten ... 21
7.3 Weitergabe von geheimen Daten ins Ausland ... 21
8. Informations-, Prüf- und Bewilligungsverfahren ... 21
Anhang zum Gutachten vom 31. Januar 2018 ... 23

1. Einleitung

1.1 Gegenstand und Adressatenkreis

Das vorliegende Gutachten analysiert die rechtlichen Rahmenbedingungen für Behörden der Kantone (Kantonsverwaltungen und Gemeinden) sowie für weitere dem kantonalen Recht unterstehende Organisationen und Unternehmen, z.B. öffentlich-rechtliche Anstalten mit eigener Rechtspersönlichkeit oder privatrechtlich organisierte Unternehmen, die öffentliche Aufgaben wahrnehmen, (nachfolgend gesamthaft auch als «öffentliche Organe» bezeichnet) im Hinblick auf die Nutzung von Cloud Services, sei es als Platform-as-a-Service (PaaS) oder Software-as-a-Service (SaaS). Nicht berücksichtigt werden Cloud Services im Servicemodell Infrastructure-as-a-Service (IaaS). Basierend auf dieser Analyse werden die Voraussetzungen für die rechtskonforme Nutzung von Cloud Services dargestellt.

Die Differenzierung zwischen PaaS und SaaS spielt dabei für die rechtliche Beurteilung keine grundsätzliche Rolle, da die massgeblichen Bestimmungen technologieneutral formuliert sind. Die Frage, ob PaaS- oder SaaS-Services bezogen werden, spielt in einem konkreten Projekt eine Rolle bei der Beurteilung der möglichen Risiken einer Weitergabe von Daten an einen Cloud-Anbieter. Im Fall von PaaS verfügt der Kunde im Vergleich zu SaaS allenfalls über mehr Möglichkeiten, um die Daten in der Cloud auf der Ebene der von ihm selbst in der Cloud betriebenen Applikationen gegen die unbefugte Kenntnisnahme durch Dritte mittels Verschlüsselung oder anderer Technologien (z.B. Trusted Execution Environment, (TEE)[1] zu schützen.

Das soben Gesagte gilt entsprechend auch mit Bezug auf die möglichen Deplyoment Modelle von Cloud Services. Die rechtlichen Fragestellungen sind im Grundsatz die gleichen, ob es um die Nutzung von Cloud Services in einer Public, Community, Private oder Hybrid Cloud geht. Auch hier zeigen sich die Unterschiede jeweils in der Beurteilung der im Zusammenhang mit einem bestimmten Deplyoment Modell für ein bestimmtes Projekt verbundenen Risiken. Diese sind tendenziell beim Modell der Public Cloud am höchsten und beim Modell der Privat Cloud am niedrigsten einzuschätzen, während die Modelle der Community Cloud und der Hybrid Cloud zwischen diesen beiden Polen liegen, und zwar je nach der jeweiligen Ausgestaltung näher bei dem einen oder anderen.

Das Gutachten richtet sie an die Verantwortlichen von öffentlichen Organen, die mit Bezug auf Cloud Projekte auch für die Berücksichtigung der rechtlichen Aspekte zuständig sind.

1.2 Zweck

Das Gutachten zeigt den allgemeinen rechtlichen Rahmen auf, wie er für Cloud Projekte von öffentlichen Organen zu berücksichtigen ist und behandelt die sich daraus ergebenden Rechtsfragen. Das Schwergewicht liegt dabei auf dem Datenschutz, der Datensicherheit, der Geheimhaltung sowie der sich daraus ergebenden Anforderungen an die Ausgestaltung des Vertragsverhältnisses mit den Anbietern von Cloud Services. Berücksichtigt werden aber auch institutionelle Gesichtspunkte, wie eine allfällige Genehmigungspflicht von Cloud Projekten. Ausgeklammert bleibt das Submissionsrecht.

Das Gutachten muss sich auf das Grundsätzliche beschränken. Die einzelnen kantonalen Rechtsordnungen weichen inhaltlich in den im vorliegenden Zusammenhang relevanten Punkten zum Teil erheblich von einander ab. Auf einzelne kantonale Regelungen kann daher nur beispielhaft eingegangen werden. Zudem lassen sich die sich stellenden Rechtsfragen nur unter Berücksichtigung der für ein konkretes Projekt massgeblichen spezifischen Gegebenheiten abschliessend beurteilen. Das Gutachten stellt somit eine Orientierungshilfe dar, um aufzuzeigen, welche rechtlichen Rahmenbedingungen typischerweise zu beachten sind und nach welchen Kriterien die sich daraus ergebenden Rechtsfragen zu beurteilen sind.

---

[1] Durch ein Trusted Execution Environment (TEE) wird eine sichere bzw. vertrauenswürdige Laufzeitumgebung für Applikationen zur Verfügung gestellt. Dabei kann auch ein Zugriff auf und damit die Kenntnisnahme der verarbeiteten Daten durch den Betreiber des Servers, auf welchem das TEE eingerichtet ist, ausgeschlossen bzw. autorisiert und kontrolliert werden.

1.3 Anhang: Checkliste

Dem dargestellten Zweck dient auch die dem Gutachten als Anhang beigefügte Checkliste.

Sie vermittelt eine strukturierte Übersicht über diejenigen Punkte, die aus rechtlicher Sicht im Zusammenhang mit einem Cloud Projekt für ein öffentliches Organ im Allgemeinen zu berücksichtigen sind. Sie kann für die Verantwortlichen in den Kantonen als Basis bzw. Hilfestellung herangezogen werden, um eine eigene, spezifisch auf die Gegebenheiten in ihrem jeweiligen Kanton abgestimmte Checklisten zu erstellen.

2. Management Summary

Zur Nutzung von Cloud-Services, sei es als PaaS oder als SaaS, sind die folgenden rechtlichen Rahmenbedingungen zu beachten:

- **Anknüpfungskriterien für die rechtlichen Regelungen:** Je nach der Gesetzgebung des einzelnen Kantons knüpfen die relevanten Bestimmungen an die Auslagerung von Informatikleistungen als solche oder aber an die Art der Daten (Personendaten, der Geheimhaltung unterliegende Daten) an.

- **Vertragliche Regelung:** Mit dem Anbieter der Cloud Lösung muss eine vertragliche Vereinbarung getroffen werden, welche sicherstellt, dass **Personendaten** vom Anbieter und seinen allfälligen Subunternehmern nur zu denjenigen Zwecken und in dem Umfang bearbeitet werden, wie dies auch für das auslagernde öffentliche Organ zulässig ist. Der Vertrag muss auch hinreichende Kontrollmöglichkeiten vorsehen, welche es der Behörde erlauben, wirksam zu überprüfen oder durch von ihr beauftragte Spezialisten überprüfen zu lassen, ob der Cloud Anbieter seine vertraglichen Pflichten einhält.

  Die kantonalen Behörden haben ferner sicherzustellen, dass die für sie geltenden Anforderungen betreffend die Datensicherheit bei der Auslagerung von Informatikleistuntgen bzw. der Bearbeitung von Personendaten auch vom Auftragsbearbeiter eingehalten werden.

  Speziell ist darauf zu achten, dass durch den Vertrag auch sichergestellt wird, dass alle vertraglichen Pflichten des Anbieters sowie vertraglichen Rechte des auslagernden öffentlichen Organs (insbesondere die Kontrollrechte) auch gegenüber allfälligen Subunternehmern des Cloud Anbieters gelten und durchgesetzt werden können.

  In einzelnen Kantonen bestehen für die Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten besondere Allgemeine Geschäftsbedingungen, die als Bestandteil des Vertrages mit dem Auftragsbearbeiter zu vereinbaren sind und die spezifische Regelungen bezüglich Datenschutz und Datensicherheit beinhalten.

- **Auslagerung ins Ausland:** Werden Daten in ein Land ausgelagert, welches über keinen angemessenen Datenschutz verfügt, so ist mit entsprechenden vertraglichen Garantien sicherzustellen, dass der Anbieter und dessen Subunternehmer für die Datenbearbeitung in dem betreffenden Land einen angemessenen Datenschutz einhalten. Auch für die kantonalen Behörden ist es dabei empfehlenswert, die Standardvertragsklauseln zu verwenden, welche von der EU-Kommission publiziert worden sind, da es sich hier um bekannte und allgemein anerkannte Regelungen handelt, welche insbesondere auch auf Seiten der Cloud-Anbieter auf Akzeptanz stossen, da sie diese bereits von den Geschäftsbeziehungen mit anderen Kunden aus dem EU/EWR-Raum kennen.

  Bei der Auslagerung der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen ins Ausland ist den damit verbundenen erhöhten Risiken, insbesondere erschwerte Kontrolle und Durchsetzung von Vertragspflichten im Ausland sowie der Möglichkeit von Datenzugriffen durch ausländische Behöreden, durch zusätzliche technische Massnahmen zu begegnen, wie insbesondere der Verschlüsselung der ins Ausland transferierten und der dort gespeicherten

Daten, da dadurch die negativen Folgen von Vertragsverletzungen durch den Cloud Services Anbeiter oder von Behördenzugriffen minimiert oder ausgeschlossen werden können.

- **Geheimhaltungspflichten:** Daten, die nicht öffentlich bekannt oder öffentlich zugänglich sind, unterstehen dem Amtsgeheimnis. Daneben bestehen eine ganze Reihe von besonderen Geheimhaltungsvorschriften, wie das Berufsgeheimnis (Art. 321 StGB) oder das Steuergeheimnis etc. Der Cloud Services Anbieter ist jeweils vertraglich auf die Einhaltung der Geheimhaltungsbestimmungen zu verpflichten, sofern dies nicht bereits durch die jeweiligen Geheimhaltungsvorschriften von Gesetzes wegen der Fall ist (wie z.B. beim Berufsgeheimnis für Hilfspersonen). Auch bei geheimen Daten ist, wie bei der Auslagerung der Bearbeitung von Personendaten, den erhöhten Risiken Rechnung zu tragen, wenn die Auslagerung ins Ausland erfolgt.

- **Melde-, Prüf- und Genehmigungsverfahren:** Je nach kantonaler Gesetzgebung unterliegt die Auslagerung von Informatikleistungen der Genehmigungspflicht. Weiter sind im Recht vieler Kantone Vorabkontrollverfahren vorgesehen, wonach je nach der von einem Projekt betroffenen Daten (besonders schützenswerte Personendaten, geheime Daten) oder den mit einem Projekt verbundenen Risiken (grosse Zahl der betroffenen Personen, technische Risiken) das Projekt der kantonalen Datenschutzaufsichtsstelle zur Prüfung zu unterbreiten ist. Häufig ist sodann im kantonalen Recht vorgesehen, dass bei einer Gewährleistung eines ausreichenden Datenschutzes im Ausland durch vertragliche Garantien (weil im Land, in welchem die Bearbeitung von Personendaten kein hinreichender gesetzlicher Datenschutz besteht), diese Garantien der kantonalen Datenschutzaufsichtsstelle zu melden sind.

3. Rechtliche Rahmenbedingungen - Übersicht

3.1 Kantonale Gesetzgebung

Rechtliche Vorgaben, welche im Zusammenhang mit der Nutzung von Cloud-Services zu berücksichtigen sind, finden sich im kantonalen Recht insbesondere in der kantonalen Datenschutzgesetzgebung sowie in der Gesetzgebung betreffend den Einsatz von Informatikmitteln und betreffend die Informationssicherheit.

Beispiel Kanton Bern:
- Datenschutzgesetz (KDSG) vom 19.2.1986
- Datenschutzverordnung (DSV) vom 22.10.2008
- Direktionsverordnung über Informationssicherheit und Datenschutz (ISDS DV) vom 3.1.2011
- Allgemeine Geschäftsbedingungen des Kantons Bern über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen (AGB ISDS), Version vom 24.3.3015

Daneben sind je nach Kanton weitere bereichsspezifische Regelungen zu berücksichtigen, die Vorgaben für die Nutzung von Cloud Services beinhalten können, z.B. Regelungen betreffend das kantonale Personalrecht oder das Gesundheitsrecht.

Aus solchen Regelungen kann sich allenfalls ergeben, dass neben den allgemeinen datenschutzrechtlichen Grundsätzen spezifische Anforderungen an die Auslagerung von Informatikleistungen bestehen, wonach z.B.
- der technische Betrieb von Informationssystemen zwingend durch eine kantonale Stelle selbst zu erfolgen hat, somit eine Auslagerung an einen Cloud Services Anbieter ausgeschlossen ist, oder dass
- für bestimmte Arten von Systemen spezifische technische oder organisatorische Anforderungen bestehen, welche daher auch im Rahmen der Nutzung einer Cloud Lösung zu erfüllen sind.

Beispiele:
- **Kanton Graubünden:** Gemäss Art. 11 der Verordnung über den Einsatz der Informatik in der Verwaltung können Informatik-Leistungen unter Berücksichtigung der Wirtschaftlichkeit, der Sicherheit und des Datenschutzes, verwaltungsintern oder –extern bezogen werden. Der Regierungsrat regelt, welche Leistungen die kantonalen Informatikbetreibenden erbringen müssen und bei diesen zu beziehen sind.
- **Kanton Thurgau:** Im Kanton Thurgau ist gemäss § 9 des Reglementes des Regierungsrates über den Einsatz der Informatik die Verwendung von fremder Hard- und Software, d.h. Hard- und Software, an welcher dem Kanton keine Eigentums- oder Nutzungsrechte zustehen, nur mit der Bewilligung des Amtes für Informatik zulässig.
- **Kanton Luzern**: Die Verordnung zum Personalgesetz sieht in § 61a vor, dass Informatikleistungen, welche das Personalinformationssystem betreffen, ausgelagert werden können, und regelt die dabei zu beachtenden Bedingungen, wie die Anforderungen an den mit dem externen Auftragnehmer abzuschliessenden Vertrag, die dem Auftragnehmer zu überbindenden Pflichten, insbesondere betreffend die Geheimhaltung, den Datenschutz und die Informationssicherheit, die Kontrolle des Auftragnehmers durch die kantonalen Behörden sowie die Pflicht zur Genehmigung von Auslagerungen durch den Regierungsrat.

3.2 Datenschutzgesetz des Bundes

Das Bundesgesetz über den Datenschutz (DSG) findet auf die Tätigkeit kantonaler öffentlicher Organe grundsätzlich keine Anwendung. Der Bund hat keine Kompetenz, die Tätigkeit der kantonalen öffentlichen Organe zu regeln. Eine Ausnahme bildet Art. 37 DSG, wonach die Kantone beim Vollzug von Bundesrecht die dort genannten Bestimmungen zu beachten sowie ein Kontrollorgan einzurichten haben, welches die Einhaltung des Datenschutzes kontrolliert. Da heute alle Kantone über ein eigenes Datenschutzgesetz verfügen, ist die Bedeutung dieser Bestimmung gering. Aktuelle Anwendungsfälle sind keine bekannt.

Eine weitere Ausnahme besteht dann, wenn sich kantonale öffentliche Organe am privaten wirtschaftlichen Wettbewerb beteiligen und somit ihre Tätigkeit nicht in Ausübung hoheitlicher Funktionen oder der Ausübung öffentlicher Aufgaben des kantonalen Rechts erfolgt[2], wie dies z.B. für die Kantonalbanken der Fall ist.

3.3 Geheimhaltungspflichten

Zu beachten sind weiter die für kantonale öffentliche Organe geltenden Geheimhaltungspflichten. Diese können im Bundesrecht vorgesehen sein, wie das allgemeine Amtsgeheimnis und das medizinische Berufsgeheimnis gemäss Art. 320 bzw. Art. 321 des Schweizerischen Strafgesetzbuches.

Weitere Geheimhaltungsbestimmungen des Bundesrechts, welche für kantonale öffentliche Organe Geltung haben, wenn sie in der Ausführung der entsprechenden Gesetze tätig sind, sind z.B. das Sozialversicherungsgeheimnis gemäss Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrecht (ATSG) oder die Schweigepflicht gemäss Art. 11 des Opferhilfegesetzes (OHG).

Das kantonale Recht sieht ebenfalls Geheimhaltungsbestimmungen vor, wie zum Beispiel die Geheimhaltungspflicht gemäss den kantonalen Steuergesetzen, sowie Geheimhaltungspflichten im Rahmen der Vorbereitung und Durchführung von Wahlen und Abstimmungen etc.

[2] Vgl. zum Beispiel Art. 4 Abs. 2 lit. a Datenschutzgesetz (KDSG) des Kantons Bern; § 2 Abs. 2 lit. a des Gesetzes über die Information und den Datenschutz (IDG) des Kantons Zürich; § 2 Abs. 2 lit. a Gesetzes über die Information und den Datenschutz (IDG) des Kantons Basel-Stadt.

3.4 Exkurs: EU-DSGVO

3.4.1 Grundsatz – keine Geltung für Schweizer Behörden

Bekanntlich wurde das Datenschutzgesetz in der EU grundlegend überarbeitet. Diese Revision umfasst zwei Rechtsakte, einmal die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgrundverordnung, DSGVO), zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts.

Nur die erwähnte Richtlinie ist Teil des Schengen-Acquis und wird von der Schweiz im Rahmen der laufenden Revision des Datenschutzgesetzes des Bundes übernommen und dann auch für die kantonalen öffentlichen Organe, die im Bereich des Strafrechts tätig sind, relevant werden.

Die Datenschutzgrundverordnung ist dagegen für kantonale öffentliche Organe grundsätzlich nicht relevant. Die EU kann basierend auf den entsprechenden EU-Rechtsakten für die öffentlichen Organe der ihr angehörenden Mitgliedstaaten verbindliche Rechtsvorschriften erlassen. Das gilt jedoch nach allgemeinen Grundsätzen des Völkerrechts nicht für die öffentlichen Organe von Drittstaaten. Auch das bisher in den EU-Staaten geltende Datenschutzrecht hatte keine Geltung für die ausländischen öffentlichen Organe. Mit der Datenschutzgrundverordnung hat sich diesbezüglich nichts geändert.

3.4.2 Ausnahmen bei privatrechtlicher Tätigkeit

Eine Ausnahme besteht dort, wo kantonale öffentliche Organe nicht hoheitlich im Rahmen ihrer öffentlichen Aufgaben, sondern rein privatrechtlich tätig sind. In diesem Bereich gelten für diese die gleichen Datenschutzregeln wie für Private. Die kantonale Gesetzgebung sieht für diesen Fall regelmässig auch eine explizite Ausnahme von der Geltung des kantonalen Datenschutzrechts vor (vgl. oben Ziff. 3.2).

Ein Beispiel für eine rein privatrechtliche Tätigkeit liegt vor, wenn schweizerische Spitäler ausländische Privatpatienten behandeln. Sind in solchen Fällen die Anknüpfungskriterien der DSGVO erfüllt, findet diese auf die betreffenden Spitäler Anwendung.

Das primäre Anknüpfungskriterium der DSGVO besteht darin, dass im Zusammenhang mit der Tätigkeit einer sich in der EU befindlichen Niederlassung eine Verarbeitung von Personendaten erfolgt[3]. Falls daher ein öffentliches Unternehmen, wie z.B. die Elektrizitätswerke des Kantons Zürich oder die IWB Basel, neben den Tätigkeiten im Rahmen des öffentlichen Versorgungsauftrages auch noch rein privatwirtschaftliche Tätigkeiten ausüben, und dabei über Niederlassungen in der EU verfügen sollten, so unterstehen sie für die Verarbeitung von Personendaten im Rahmen der Tätigkeiten dieser Niederlassungen der DSGVO, und zwar selbst dann, wenn die eigentliche Verarbeitung der Personendaten nicht in der betreffenden EU-Niederlassung, sondern in der Schweiz erfolgen sollte.

Das zweite Anknüpfungskriterium beruht auf dem sogenannten Marktortprinzip[4]. Danach ist die DSGVO anwendbar, wenn betroffenen Personen, die sich in der EU aufhalten, Angebote von Waren oder Dienstleistungen gemacht werden. Ein Spital, welches Personen, die sich in der EU befinden, medizinische Behandlungen anbietet, untersteht somit im Zusammenhang mit diesen Aktivitäten der DSGVO, da diese Behandlungen nicht in den Rahmen der Erfüllung der Gesundheitsversorgung gemäss dem kantonalen Gesundheitsrecht fallen und damit nicht in der Erfüllung einer öffentlichen Aufgabe erfolgen.

Das dritte Anknüpfungskriterium ist Beobachtung des Verhaltens von Personen, sofern das beobachte Verhalten in der EU erfolgt[5]. Relevant ist dabei lediglich das Beobachten des Verhaltens Betroffener im

[3] Art. 3 Abs. 1 DSGVO

[4] Art. 3 Abs. 2 lit. a DSGVO

[5] Art. 3 Abs. 2 lit. b DSGVO

Internet. Das ergibt sich zwar nicht aus dem Wortlaut der EU-DSGVO selbst, jedoch aus den zusammen mit dieser veröffentlichen Erwägungsgründen.

Die Geltung der DSGVO, basierend auf dem Kriterium der Verhaltensbeobachtung, kommt für öffentliche Unternehmen und Organisationen allenfalls dann in Frage, wenn auf deren Website im Zusammenhang mit einer allfälligen privatrechtlichen Tätigkeit Daten von Internetnutzern, die sich in der EU befinden, erhoben und ausgewertet werden, z.B. Aufzeichnungen des Datenverkehrs auf der Website (Webtracking) mittels Logdateien des Webservers oder anderen Methoden (Tags, Pixels etc.) oder mittels Cookies.

Voraussetzung ist allerdings, dass die Möglichkeit besteht, die so erhobenen Daten bestimmten natürlichen Personen zuzuordnen. Dies ist für Daten aus der Aufzeichnung des Datenverkehrs, aber auch für mittels Cookies erhobene Daten, in der Regel nicht möglich. Wenn sich jedoch z.B. Besucher der Website unter Angabe ihrer Personalien registrieren können, so wäre es möglich, für die registrierten Benutzer die im Rahmen des Registrierungsprozesses angegeben Daten mit den Daten, die mittels Cookies erhoben wurden, zu kombinieren, womit der Personenbezug hergestellt ist. Dann läge eine Verhaltensbeobachtung im Sinne der DSGVO vor.

Kein Anknüpfungspunkt für die DSGVO ist dagegen die Beschäftigung von Personen mit EU-Bürgerrecht oder EU-Domizil.

4. Datenschutz

Im Zentrum der Frage nach der rechtlichen Zulässigkeit der Auslagerung von Informatikdienstleistungen in die Cloud steht der Datenschutz.

4.1 Personendaten

Die einzelnen kantonalen Gesetzgebungen mögen im Wortlaut Abweichungen aufweisen. Trotzdem kann davon ausgegangen werden, dass der zentrale Begriff der «Personendaten», an welchen der Datenschutz anknüpft, überall der gleiche ist. Es sind darunter alle Angaben zu verstehen, welche sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.

Beispiel:
- **Kanton Bern:** «Personendaten sind Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person.» (Art. 2 Abs. 1 KDSG)

Anzumerken ist, dass in der Gesetzgebung verschiedener Kantone der Datenschutz und die Regelung des Öffentlichkeitsprinzips im gleichen Erlass erfolgt[6]. Der zentrale Anknüpfungspunkt ist in diesen Fällen der Begriff der «Information». Die Personendaten stellen in dieser Systematik dann eine Untermenge der Informationen dar.

Bei der Anwendung dieser Gesetzte ist jeweils zu berücksichtigen, ob eine bestimmte Norm allgemein für Informationen oder aber nur für Personendaten gilt[7].

4.2 Besondere Kategorien von Personendaten

Unter den Oberbegriff der Personendaten fallen ferner die folgenden besonderen Kategorien von Personendaten, für die teilweise strengere datenschutzrechtliche Anforderungen gelten:

---

[6] So z.B. je in den Gesetzen über die Information und den Datenschutz (IDG) der Kantone Zürich und Basel-Stadt.

[7] So regelt z.B. § 7 IDG des Kantons Basel-Stadt die Bearbeitung von Informationen im Auftrag eines öffentlichen Organs, während § 23 IDG die grenzüberschreitende Bekanntgabe ausschliesslich von Personendaten zum Gegenstand hat.

- **«besonders schützenswerte Personendaten»**, das heisst Daten 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, sowie
- **«Persönlichkeitsprofile»**, das heisst Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Personen erlauben[8].

Beispiel:
- **Kanton Wallis:** Art. 2 Abs. 7 und 8 des Gesetzes über die Information und Öffentlichkeit, den Datenschutz und die Archivierung (GIDA):
  [7] Besonders schützenswerte Daten: Personendaten über
  a) die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten;
  b) die Gesundheit, die Intimsphäre oder die rassische Zugehörigkeit;
  c) Sozialhilfemassnahmen;
  d) straf- und verwaltungsrechtliche Verfolgungen oder Sanktionen.

  [8] Persönlichkeitsprofil: eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

4.3 Entpersonalisierung von Daten (Anonymisierung, Pseudonymisierung, Verschlüsselung)

4.3.1 Rechtliche Relevanz

Die rechtliche Relevanz der verschiedenen Methoden zur Entpersonalisierung von Daten (Anonymisierung, Pseudonymisierung, Verschlüsselung[9]) besteht darin, dass die Daten wegen des fehlenden bzw. nicht erkennbaren Bezugs der Daten zu bestimmten oder zu bestimmbaren Personen nicht mehr den Anforderungen des Datenschutzes unterliegen.

Im Zusammenhang mit den Geheimhaltungspflichten verhindert die Verschlüsselung, dass der Inhalt der Daten von Dritten, die nicht über den kryptographischen Schlüssel verfügen, zur Kenntnis genommen werden kann und daher bei der Weitergabe von verschlüsselten Daten keine die Geheimhaltungspflicht verletzende Offenbarung vorliegt. Dort, wo das Geheimhaltungsinteresse, wie z.B. beim medizinischen Berufsgeheimnis, darin liegt, dass Daten keiner bestimmten oder bestimmbaren Person zugeordnet werden können, kann die Offenbarung des geheimzuhaltenden Sachverhalts (der Personenbezug) ebenfalls durch Pseudonymisierung verhindert werden.

4.3.2 Anonymisierung

Anonymisierte Daten stellen keine Personendaten im Sinne des Datenschutzes dar. Bei der Anonymisierung werden die Daten irreversibel von jedem Personenbezug befreit. Die Daten können keinen Personen mehr zugeordnet werden und es gibt (im Unterschied zur Pseudonymisierung) keine Möglichkeit mehr, den Personenbezug wiederherzustellen. Die Anonymisierung kommt daher nur in relativ wenigen Fällen in Frage, wenn nämlich der Personenbezug für die vorgesehenen Verwendungszwecke der Daten keine Rolle spielt, z.B. wenn Personendaten für gewisse statistische Zwecke aufbereitet werden. Zu beachten ist, dass die Anonymisierung häufig vom aktuellen Stand der Technik und

[8] Die Begrifflichkeit ist allerdings nicht immer einheitlich. So kennt § 3 Abs. 4 lit. a IDG des Kantons Zürich die Definition der „besonderen Personendaten", worunter einerseits Informationen zu verstehen sind, bei denen aufgrund ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönllichkeitsverletzung besteht. Die oben im Text erwähnten besonders schützenswerten Personendaten werden dann als Beispiele aufgeführt. Ferner beinhaltet die Definition der „besonderen Personendaten" gemäss § 3 Abs. 4 lit. b IDG auch Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben, was den oben im Text erwähnten Persönlichkeitsprofilen entspricht.

[9] Dabei ist zu beachten dass bei sämtlichen kryptografischen Tätigkeiten in der Cloud u. A.. die sog. "logische Sekunde" (Quelle: Wikipedia) oder andere Schwachstellen bei der genutzten Lösung nicht eintreten können. Dies würde der Schutz der betroffenen Daten massiv in Frage stellen.

deren absehbaren Entwicklung abhängig ist. Es ist nicht ausgeschlossen, dass Daten, die zu einem bestimmten Zeitunkt als hinreichend anonymisiert gelten, später wieder re-personalisiert werden können. Diese Problematik wird insbesondere bei der Diskussion des Datenschutzes im Rahmen von Big Data diskutiert.

4.3.3 Pseudonymisierung

Anders als bei anonymisierten Daten ist bei pseudonymisierten Daten ein Personenbezug vorhanden, dieser ist jedoch bei korrekter Pseudonymisierung für Dritte nicht erkennbar. Bei der Pseudonymisierung werden die personenbezogenen Merkmale durch Platzhalter ersetzt, z.B. Namen durch eine Kennziffer, so dass für Dritte die Daten keinen Rückschluss mehr auf eine bestimmte Person gestatten. Der Inhaber der Daten kann demgegenüber mittels eines Schlüssels den Personenbezug wieder herstellen.

Die Problematik bei der Pseudonymisierung liegt darin, dass die Aufhebung des Personenbezugs häufig nur graduell und nicht absolut möglich ist. Werden z.B. die Patientennamen durch eine Kennzahl ersetzt, so ist dies in den meisten Fällen noch nicht ausreichend, da die Daten noch genügend andere individualisierende Merkmale aufweisen, welche die personenbezogene Zuordnung, wenn vielleicht auch nicht in allen, so jedoch nach wie vor in vielen Fällen erlauben. Andererseits ist zu berücksichtigen, dass ein aussenstehender Dritter nicht über das gleiche Hintergrundwissen verfügt, wie Personen aus dem näheren Umfeld der betroffenen Person, z.B. Angehörige des medizinischen Behandlungsteams oder Familienangehörige, welchen ihr Hintergrundwissen, trotz Pseudonymisierung der Daten, noch eine indivdiuelle Zuordnung ermöglicht.

Zu prüfen ist daher jeweils im Einzelfall, welches Risiko besteht, dass Personen Zugriff auf die pseudonymisierten Daten erhalten könnten, welche aufgrund ihrer Hintergrundkenntnisse in der Lage sind, die Daten bestimmten Personen zuzuordnen. Erscheint dieses Risiko nach den Umständen als zumutbar gering, ist die Pseudonymisierung genügend, um die Daten im Verhältnis zu Dritten, welche nicht über den Schlüssel für die Zuordnung der Daten zu individuellen Personen verfügen, ebenfalls wie anonymisierte Daten zu behandeln. Das heisst, die Bestimmungen des Datenschutzrechts finden bei ausreichend pseudonymisierten Daten keine Anwendung, da es für Dritte nicht möglich ist, die Daten ohne einen nach den Umständen nicht zu erwartenden, unangemessen hohen Aufwand individualisierbaren Personen zuzuordnen.

4.3.4 Verschlüsselung

Wie für pseudonymisierte Daten gilt auch in Bezug auf verschlüsselte Daten, dass bei einer unter den gegebenen Umständen genügend starken Verschlüsselung davon ausgegangen werden kann, dass Dritte mit zumutbarem Aufwand die Daten nicht zur Kenntnis nehmen und den Bezug zu bestimmten oder bestimmbaren Personen nicht herstellen können. Die verschlüsselten Daten unterliegen daher im Verhältnis zu Dritten, welche nicht über den Schlüssel verfügen, nicht den Regeln des Datenschutzrechts.

5. Datenbearbeitung durch Dritte (Auftragsdatenbearbeitung)

5.1 Allgemein – Grundsätzliche Zulässigkeit

Die kantonalen Gesetzgebungen sehen jeweils vor, dass die Bearbeitung von Informationen oder Personendaten[10] an Dritte ausgelagert werden kann.

Beispiele:
- **Kanton Bern KDSG:**
  Art. 16 Bearbeiten im Auftrag

[10] Zur Unterschiedlichen Anknüpfung der gesetzlichen Regelungen in den verschiedenen Kantonen vgl. oben Ziff. 4.1.

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.

- **Kanton Wallis GIDA:**
  Art. 29 Bearbeiten im Auftrag
  Beauftragt der Inhaber der Datensammlung einen Dritten mit dem Bearbeiten von Daten, muss er dafür sorgen, dass der Schutz dieser Informationen und des Bearbeitungsergebnisses gemäss den obengenannten Bestimmungen gewährleistet ist.

- **Kanton Basel-Stadt IDG:**
  §7 Bearbeiten im Auftrag
  [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.

Aufgrund dieser Bestimmung ist die Auslagerung der Bearbeitung von Informationen bzw. Personendaten durch öffentliche Organe an Dritte grundsätzlich zulässig. Die Zustimmung der betroffenen Personen ist dabei nicht erforderlich.

Auch wenn dies aus dem Wortlaut der jeweiligen kantonalen Bestimmungen nicht immer unmittelbar hervorgeht, so ist anerkannt, dass für die Auslagerung der Bearbeitung von Informationen/Personendaten die folgenden Grundsätze zu gelten:

- Die Auslagerung ändert nichts daran, dass das öffentliche Organ, welches einen Dritten mit der Bearbeitung von Personendaten beauftragt, nach wie vor die volle Verantwortung für die Datenbearbeitung hat.
- Das öffentliche Organ hat insbesondere sicherzustellen, dass der beauftragte Dritte die Informationen/Daten nur so bearbeitet, wie es das auftraggebende öffentliche Organ selbst darf.
- Das auslagernde öffentliche Organ hat weiter dafür zu sorgen, dass die Datensicherheit beim beauftragten Dritten gewährleistet ist.
- Die Auslagerung der Datenbearbeitung an einen Dritten darf ferner nur erfolgen, wenn dadurch keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden.

In den nachfolgenden Kapiteln wird im Einzelnen auf die genannten Voraussetzungen für eine zulässige Auftragsdatenbearbeitung eingegangen.

Je nach Kanton finden sich Regelungen betreffend die Auslagerung der Bearbeitung von Informationen/Personendaten oder generell betreffend die Auslagerung von Informatikleistungen unter Umständen nicht nur im kantonalen Datenschutzrecht, sondern in bereichsspezifischen Regelungen wie dem Gesundheitsrecht oder den kantonalen Bestimmungen über den Informatikeinsatz.

Beispiele:

- **Kanton Bern Verordnung und Pflichten der Patientinnen und Patienten und der Gesundheitsfachpersonen (PatV):**
  Art. 12 Elektronische Datenbearbeitung durch Dritte
  [1] Werden zur elektronischen Datenverarbeitung Personen oder Organisationen beigezogen, die nicht der Institution angehören (Outsourcing), so muss die Institution mit den beauftragten Personen und Organisationen einen schriftlichen Vertrag über die Datenbearbeitung abschliessen.
  [2] Der Vertrag muss insbesondere folgende Punkte enthalten:
  a Umfang der Datenbearbeitung,
  b Bestimmungen über die Schweigepflicht,
  c Auflagen und Vereinbarungen betreffend Datensicherheit und Datenschutz.
  [3] Die Gesundheits- und Fürsorgedirektion kann Vorschriften über die Aufnahme bestimmter Vertragsbestimmungen erlassen.

- **Kanton Luzern Informatikgesetz:**
  § 13Zulässigkeit
  [1] Die Auslagerung von Informatikdienstleistungen ist zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Die finanzrechtlichen Vorschriften bleiben vorbehalten.
  [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.
  [3] Das auslagernde Organ stellt durch organisatorische oder technische Massnahmen sowie vertraglich sicher, dass die staatliche Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.

5.2 Bearbeitung wie der Auftraggeber

Das öffentliche Organ, welches Daten zur Auftragsbearbeitung an einen Dritten weitergibt, hat sicherzustellen, dass der Dritte die Daten nur so bearbeitet, wie es für die auftraggebende öffentliche Organe selbst zulässig ist.

5.2.1 Vertragliche Vereinbarung notwendig

Unabhängig davon, ob das kantonale Recht spezifische Vorgaben[11] in Bezug auf die mit einem Auftragsdatenbearbeiter zu treffenden vertraglichen Vereinbarungen macht oder nicht, ist nach allgemeiner Auffassung der Abschluss eines schriftlichen Vertrages notwendig. Ohne schriftlichen Vertrag ist das öffentliche Organ nicht in der Lage, die trotz der Auslagerung an einen Dritten bei ihr verbleibende Verantwortung für die Datenbearbeitung wahrzunehmen.

Schriftlich heisst nicht zwingend Schriftlichkeit im Sinne der gegenseitigen Unterzeichnung durch die Parteien. Wenn die getroffene Vereinbarung in Schriftform nachweisbar ist, ist dies genügend. So können etwa auch Dokumente wie Allgemeine Geschäftsbedingungen etc. Bestandteil des Vertrages sein, die nicht unterzeichnet werden. Es muss jedoch durch eine entsprechende Referenzierung und Versionierung eindeutig feststellbar sein, in welcher Fassung diese Dokumente vereinbart worden sind.

Folgende Punkte sind im Vertrag mit dem Auftragsdatenbearbeiter zu regeln:

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortlichkeiten der an der Vertragsdurchführung beteiligten Stellen/Personen der Vertragsparteien
- Verfügungsmacht des Auftraggebers über die Daten
- Zweckbindung der Datenbearbeitung durch den beauftragten Dritten
- Weisungsrecht des Auftraggebers mit Bezug auf die Bearbeitung der Personendaten durch den beauftragten Dritten
- Festlegung der Zugriffsberechtigungen des beauftragten Dritten bzw. von dessen Mitarbeitenden auf die Daten
- Voraussetzungen für eine allfällige Bekanntgabe der Daten durch den beauftragten Dritten
- Geheimhaltungsverpflichtungen

[11] Vgl. neben den oben erwähnten Beispielen des Informatikgesetzes des Kantons Luzern und der Patientenrechtsverordnung des Kantons Bern z.B. auch § 25 der Verordnung über die Information und den Datenschutz (IDV) vom 28.5.2008 des Kantons Zürich.

- Vorgehen im Zusammenhang mit der Wahrnehmung der Rechte durch die betroffenen Personen (Auskunft, Berichtigung, Löschung, Sperrung)
- Organisatorische und technische Massnahmen zur Wahrung des Datenschutzes und der Datensicherheit
- Kontrollmöglichkeiten des Auftraggebers bzw. Prüfungen durch Dritte (Audits) zur Zurverfügungstellung der Auditberichte an den Auftraggeber
- Informationspflicht des Auftragsdatenbearbeiters gegenüber dem Auftraggeber bei Verletzungen des Datenschutzes (Data Breaches)
- Regelung des Beizugs/Wechsels von Subunternehmern, das heisst, es muss sichergestellt sein, dass für die Subunternehmer die mit dem Cloud Anbieter vereinbarten vertraglichen Pflichten ebenfalls gelten und ebenfalls alle gesetzlichen Anforderungen erfüllt sind[12]
- Ort(e) der Datenbearbeitung, das heisst Standort(e) der Server
- Haftung / Konventionalstrafen
- Vertragsdauer und -auflösung
- Folgen der Vertragsauflösung (Rückführung der Daten, Löschung auf den Systemen des beauftragten Dritten)
- Anwendbarkeit von Schweizer Recht und Gerichtsstand in der Schweiz.

5.2.2 Besondere Vertragsbedingungen

Wie bereits gesehen[13] bestehen je nach Kanton gesetzliche Regelungen, welche Vorgaben bezüglich des Inhalts des Vertrages mit dem Auftragsbearbeiter machen. In gewissen Kantonen bestehen jedoch auch Allgemeine Geschäftsbedingungen, welche als Bestandteil von Verträgen zur Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten mit den Auftragsbearbeitern vereinbart werden müssen.

Beispiele:

- **Kanton Bern:**
  Im Kanton Bern hat das Amt für Informatik und Organisation gestützt auf die Direktionsverordnung über Informationssicherheit und Datenschutz die Allgemeinen Geschäftsbedingungen des Kantons Bern über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen (AGB ISDS) erlassen. Zurzeit gilt die Version V3.0 vom 24.3.2015[14]. Sie gelten für die der genannten Verordnung unterstellten Stellen, das heisst, die Kantonsverwaltung sowie für weitere Stellen, für welche das kantonale Datenschutzgesetz gilt, wenn sie vom Kanton Beiträge für ein Informatikprojekt erhalten.

  Die AGB ISDS regeln die für das Vertragsverhältnis mit dem Auftragsdatenbearbeiter massgeblichen Grundsätze betreffend den Datenschutz und die Datensicherheit.

- **Kanton Zürich**
  Im Kanton Zürich bestehen die vom Regierungsrat beschlossenen und verbindlich vorgegebenen Allgemeinen Geschäftsbedingungen (AGB) bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatik) vom 14.6.2015[15].

[12] Befindet sich ein Subunternehmer z.B. in einem Land, in dem kein angemessener Datenschutz besteht, so muss durch entsprechende vertragliche Garantien ein gleichwertiger Datenschutz gewährleistet werden; vgl. dazu im Einzelnen unten Ziff. 6.1, Seite 17ff.

[13] Vgl. oben Ziff. 5 die Beispiele der Patientenrechtsverordnung des Kantons Bern sowie des Informatikgesetzes des Kantons Luzern und der Verordnung zum Personalgesetz des Kantons Luzern.

[14] Die AGB ISDS sind zu finden auf der Website der kantonalen Finanzdirektion unter http://www.fin.be.ch/fin/de/index/informatik/informatik/rechtliche_grundlagen/ISDS.html

[15] Die AGB Auslagerung Informatik sind unter http://www.kitt.zh.ch/internet/finanzdirektion/kitt/de/it_sicherheit.html auf der Website der kantonalen Finanzdirektion publiziert.

Diese AGB müssen von allen öffentlichen Organen, soweit sie dem IDG unterstehen[16], als Bestandteil des Vertrages mit dem Auftragsdatenbearbeiter vereinbart werden. Sie regeln, wie die AGB ISDS des Kantons Bern, die Grundsätze betreffend den Datenschutz und die Datensicherheit.

- **Kanton Solothurn**
  Im Kanton Solothurn gelten basierend auf einem Beschluss des Regierungsrates[17] die Allgemeinen Geschäftsbedingungen des Kantons Solothurn über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen (AGB ISDS). Sie gelten für die kantonale Verwaltung, die Polizei und die Gerichte. Keine Geltung haben sie für die Solothurner Spitäler AG, die Fachhochschule Nordwestschweiz und die kantonalen Anstalten.

Die kantonalen AGBs beinhalten verschiedene Bestimmungen, die üblicherweise durch die Standardvertragsbedingungen der Anbieter von Cloud Services nicht abgedeckt sind oder dazu im Widerspruch stehen. Sofern ein Cloud Services Anbieter nicht bereit ist, solche weiterghenden Bedingungen zu akzeptieren, muss jeweils geprüft werden, ob es sich unter Beachtung der spezifischen Gegebenheiten eines bestimmten Projektes rechtfertigen lässt, eine Ausnahme von den kantonalen AGB zu machen, und ob eine solche Ausnahme gemäss dem anwendbaren kantonalen Recht zulässig ist.

Beispiele:

- **Aufsicht und Kontrolle:**
  Die kantonalen AGBs sehen jeweils vor, dass der Auftragnehmer der Aufsicht und Kontrolle der für das auftraggebende kantonale öffentliche Organ zuständigen Aufsichtsbehörde(n), wie Datenschutzstelle, Informationssicherheitsstelle oder Finanzkontrolle, untersteht und den Aufsichtsbehörden zur Durchführung von Kontrollen Auskünfte zu erteilen sowie Zutritt und Unterstützung zu gewähren hat.[18]

- **Einbindung von Mitarbeitenden und Subunternehmern**:
  Die AGB Auslagerung Informatikleistungen des Kantons Zürich sehen nicht nur vor, dass der Auftragnehmer, dessen Mitarbeitende, Hilfspersonen und Subunternehmer der Geheimhaltungs- und Schweigepflicht gemäss dem Amtsgeheimnis oder sonstigen Geheimhaltungsbestimmungen unterstehen, sondern dass das auftraggebende öffentliche Organ gegenüber den Mitarbeitenden das Auftragnehmers sowie der Subunternehmer und allfälligen weiteren Hilfspersonen des Auftragnehmers und gegenüber allfälligen Subunternehmern, welche besonders schützenswerte Personendaten bearbeiten, ein unmittelbares Kontroll- und Weisungsrecht hat, ausser die Kenntnisnahme von Daten durch die betreffenden Mitarbeitenden sei durch organisatorische und technische Massnahmen ausgeschlossen[19].

Die von der Schweizerischen Informatikkonferenz (SIK) herausgegebenen Allgemeinen Geschäftsbedingungen für IKT-Leistungen[20] sehen dagegen bewusst von spezifischen Regelungen mit Bezug auf die Auftragsbearbeitung, d.h. die Auslagerung von IKT-Dienstleistungen an Dritte oder die Erbringung von Cloud Services, ab. In Ziff 13.6 der AGB SIK wird ausdrücklich festgehalten, dass geltende Datenschutz- und Sicherheitsbestimmungen sowie Vorschriften betreffend die Geheimhaltung einzuhalten sind. Im Übrigen aber wird die Vereinbarung von besonderen Regelungen betreffend den Datenschutz, die Datensicherheit und die Geheimhaltung durch die Parteien ausdrücklich vorbehalten. Einzelne der vorerwähnten kantonalen AGB nehmen explizit auf die AGB SIK Bezug und füllen darin vorgesehenen Vorbehalt aus, indem sie festelegen, dass sie mit Bezug auf den Datenschutz- und die Datensicherheit an die Stelle der AGB SIK treten[21]

[16] Gemäss § 3 Abs. 1 sind dem IDG unterstellt: der Kantonsrat, die Gemeindeparlamente und –versammlungen, alle Behörden und Verwaltungen des Kantons und der Gemeinden sowie alle Organisationen und Personen des öffentlichen und privaten Rechts, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind.

[17] Regierungsratsbeschluss Nr. 2016/2093 vom 28,.11.2016, abrufbar unter http://rrb.so.ch/.

[18] Ziff. 2.9 AGB ISDS Kanton Bern; Ziff. 9b der AGB Auslagerung Informatikleistungen des Kantons Zürich; Ziff. 2.9 Abs. 4 AGB ISDS Kanton Solothurn.

[19] Ziff. 6 der AGB Auslagerung Informatikleistungen des Kantons Zürich.

[20] Massgeblich ist die Ausgabe Januar 2015; zusammen mit den entsprechenden Musterverträgen wiedergegeben auf der Website der SIK unter http://www.sik.ch/agb.html

[21] Vgl. je Ziff. 1.4 der AGB ISDS Kanton Bern und der AGB ISDS Kanton Solothurn.

5.3 Datensicherheit

5.3.1 Allgemeine Anforderungen

Wie bereits erwähnt[22], verlangt die kantonale Gesetzgebung im Zusammenhang mit der Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten dass der Auftragnehmer die Datensicherheit gewährleistet. Das auftraggebende öffentliche Organ hat somit sicherzustellen, dass der Dritte bei der Datenbearbeitung die gleichen Sicherheitsstandards einhält, wie sie für die Behörde selbst gelten.

Die kantonale Gesetzgebung definiert jedoch in aller Regel keine konkreten Schutzmassnahmen, sondern legt lediglich Grundsätze fest bezüglich der Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität), der zu berücksichtigenden Risiken (insbesondere zufällige oder unbefugte Vernichtung, zufälliger Verlust, technische Fehler, Fälschung, Diebstahl und widerrechtliche Verwendung sowie unbefugtes Ändern, Kopieren, Zugreifen und andere unbefugte Bearbeitungen) sowie bezüglich der Kriterien, nach welchen die zu ergreifenden Massnahmen zu beurteilen sind (Zweck der Datenbearbeitung, Art und Umfang der Datenbearbeitung, mögliche Risiken für die betroffenen Personen, gegenwärtiger Stand der Technik).

Im Zusammenhang mit der elektronischen Bearbeitung von Daten werden regelmässig weitere Massnahmen vorgegeben, wobei auch hier jeweils nicht die konkreten Massnahmen festgelegt werden, sondern die Ziele, welche mit den Massnahmen angestrebt werden sollen.

Beispiel:
DSV Kanton Bern
Art. 4 Grundsatz
[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). Insbesondere schützt sie 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 Massnahmen müssen angemessen sein. Insbesondere tragen sie folgenden Kriterien Rechnung:

a Zweck der Datenbearbeitung,
b Art und Umfang der Datenbearbeitung,
c Einschätzung der möglichen Risiken für die betroffenen Personen,
d gegenwärtigem Stand der Technik.

3 Die Risiken und Massnahmen sind periodisch zu überprüfen.

Art. 5 Besondere Massnahmen
[1] Die verantwortliche Behörde trifft insbesondere bei der elektronischen Bearbeitung von Personendaten die folgenden technischen und organisatorischen Massnahmen:

a Zugangskontrolle: Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;
b Personendatenträgerkontrolle: Unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
c Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beimTransport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;
d Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;
e Speicherkontrolle: Die unbefugte Eingabe in den Speicher sowie die unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;
f Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;

[22] Ziff. 5.1

g Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
h Eingabekontrolle: In automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.

[2] Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.

Im Zusammenhang mit der Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten ist vom auftraggebenden öffentlichen Organ jeweils zu prüfen, ob mit Bezug auf das jeweilige konkrete Projekt die vom Auftragnehmer getroffenen Sicherheitsmassnahmen den Grundsätzen des kantonalen Rechts bezüglich der Datensicherheit genügen.

5.3.2 Besondere Anforderungen

Insbesondere in denjenigen Kantonen, in denen Allgemeine Geschäftsbedingungen für die Auslagerung von Informatikleistungen bzw. Datenbearbeitungen bestehen, beinhalten diese regelmässig spezifische Anforderungen betreffend die Datensicherheit.

Beispiele:
- Der Auftragsnehmer hat das auftraggebende öffentlich Organ über seine Methoden und Prozesse zur Einhaltung der Informationssicherheit zu informieren. Die auftraggebende Behörde hat das Recht, weiterführende Unterlagen einzusehen und sich betriebliche Abläufe demonstrieren zu lassen.[23]
- Durch geeignete organisatorische und technische Massnahmen ist die Trennung der Datenbestände der auftraggebenden Behörde von denjenigen anderer Auftraggeber sicherzustellen.[24]
- Die auftraggebende Behörde ist über besondere Vorkommnisse (Datenverlust, Hackerangriffe, unbefugte Zugriffe etc.) zu informieren. Zwischen den Parteien sind verbindlich Meldewege festzulegen.[25]
- Der Auftragsbearbeiter ist verpflichtet, periodische Sicherheits-Audits nach anerkannten Audit-Standards durch das auftraggebende öffentliche Organ oder externe Prüfstellen durchführen zu lassen und dem auftraggebenden öffentlichen Organ die entsprechenden Berichte auf Anfrage zur Verfügung zu stellen.[26]
- Falls der Auftragsnehmer zertifiziert ist und in diesem Zusammenhang regelmässig auditiert wird, hat er die entsprechenden Berichte dem auftraggebenden öffentlichen Organ zukommen zu lassen, soweit die Reports die Bearbeitung der von dieser Behörde ausgelagerten Daten betreffen.[27]
- Der Auftragsbearbeiter hat die Massnahmen des ISDS-Grundschutzes sicherzustellen, wie sie im Anhang zu den AGB ISDS definiert sind, sowie bei erhöhten ISDS-Ansprüchen, die über den Grundschutz hinausgehen,[28] die zusätzlichen Anforderungen in einem ISDS-Konzept festzuhalten und dieses als Bestandteil des Vertrages zu erklären.[29]
- Der Auftragnehmer ist verpflichtet, ein Sicherheitsmanagement zu unterhalten, abgestimmt auf den Schutzbedarf der von ihm bearbeiteten Daten, sowie eine Sicherheitsorganisation und ein Sicherheitskonzept im Hinblick auf die Aufrechterhaltung und ständige Verbesserung der Informationssicherheit zu erstellen, wobei die Standards ISO/IEC der 27000 Serie oder des BSI[30] Grundschutzstandards 100-1 bis 100-4 massgeblich sind.[31]

---

[23] Ziff. 2.1 Abs. 1 AGB ISDS Kanton Bern; Ziff. 8c Abs. 1 AGB Auslagerung Informatikleistungen des Kantons Zürich; Ziff. 2.3 Abs. 2 AGB ISDS Kanton Solothurn.

[24] Ziff. 8b AGB Auslagerung Informatikleistungen des Kantons Zürich.

[25] Ziff. 2.1 Abs. 2 AGB ISDS Kanton Bern; Ziff. 8c Abs. 2 AGB Auslagerung Informatikleistungen des Kantons Zürich; Ziff. 2.3 Abs. 2 AGB ISDS Kanton Solothurn.

[26] Ziff. 2.8 AGB ISDS Kanton Bern; Ziff. 9a AGB Auslagerung Informatikleistungen des Kantons Zürich; Ziff. 2.9 Abs. 1 AGB ISDS Kanton Solothurn.

[27] Ziff. 2.8 Abs. 2 ABG ISDS Kanton Bern; Ziff. 2.9 Abs. 3 AGB ISDS Kanton Solothurn.

[28] Dies ist etwa der Fall, wenn besonders schützenswerte Personendaten oder der Geheimhaltung unterliegende Daten Gegenstand der Auslagerung sind, falls ein Systemausfall gravierende Folgen auf die Aufgabenerfüllung des auftraggebenden öffentlichen Organs hätte oder eine Wiederherstellung von Daten mit erheblichen Problemen oder Kosten verbunden wäre. Vgl. z.B. Art. 5 ISDS DV Kanton Bern.

[29] Ziff. 2.2 und 2.3 AGB ISDS Kanton Bern; vgl. auch Ziff. 2.4 AGB ISDS Kanton Solothurn.

[30] BSI = (deutsches) Bundesamt für Sicherheit in der Informatik.

[31] Ziff. 8a AGB Auslagerung Informatikleistungen des Kantons Zürich.

- Im Zusammenhang mit Cloud Services sind insbesondere die folgenden Anforderungen zwingend[32]:
  - Der Auftragsnehmer hat das auftraggebende öffentliche Organ umfassend über die eingesetzte Technologie und deren Weiterentwicklung zu informieren.
  - Das auftraggebende öffentliche Organ ist über sämtliche mögliche Datenbearbeitungsorte zu informieren.
  - Datenbestände mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen[33] dürfen nur mit einer «umfassenden kryptographischen» Sicherung in die Cloud transferiert und dort gespeichert werden, wobei Voraussetzung ist, dass die Zertifikate von der auftraggebenden Behörde verwaltet werden.

Falls ein Cloud-Anbieter nicht bereit ist, solche weitergehenden Bedingungen für sich zu akzeptieren muss jeweils geprüft werden, ob es sich unter Beachtung der spezifischen Gegebenheiten eines bestimmten Projektes rechtfertigen lässt, eine Ausnahme von den kantonalen AGB zu machen, und ob eine solche Ausnahme gemäss dem anwendbaren kantonalen Recht zulässig ist.

6. Weitergabe ins Ausland

6.1 Anforderungen gemäss Datenschutzrecht

Falls der Auftragsdatenbearbeiter sich im Ausland befindet, kommen neben den Bestimmungen betreffend die Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten nach herrschender Auffassung zusätzlich auch die besonderen datenschutzrechtlichen Regelungen betreffend die Weitergabe von Personendaten ins Ausland zur Anwendung.

Danach dürfen Personendaten nicht ins Ausland weitergegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, insbesondere, wenn im Empfängerland keine Gesetzgebung besteht, welche einen angemessenen Datenschutz gewährleistet.

Beispiele:
Kanton Bern:
Art. 14a Abs. 1 KDSG
[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.

Kanton Luzern:
Art. 12a Abs. 1 DSG
[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.

Teilweise wird jedoch auch die Auffassung vertreten, dass die Regelungen über die Bekanntgabe von Personendaten im Falle der Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten nicht zur Anwendung kommen, weil es sich hier eben nicht um eine echte Bekanntgabe von Personendaten an Dritte handle, da bei der Auslagerung die Daten vom Dritten ja im Auftrag und für Zwecke des auftraggebenden öffentlichen Organs bearbeitet werden und nicht für eigene Zwecke des Dritten.[34] Trotzdem wird jedoch auch nach dieser Auffassung eine analoge Anwendung der Bestimmung bezüglich der Datenbekanntgabe ins Ausland gefordert.[35]

---

[32] Ziff. 13 AGB Auslagerung Informatikleistungen des Kantons Zürich.

[33] Das IDG des Kantons Zürich fasst beides unter dem Begriff „besondere Personendaten" zusammen; vgl. § 3 Abs. 3 lit. a und b IDG.

[34] Vgl. B. Baeriswyl/B. Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich 2012, Rz. 5 und 27 zu § 6, oder B. Rudin/B. Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Rz. 12ff zu § 7.

[35] Vgl. B. Baeriswyl/B. Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich 2012, Rz. 27 zu § 6, und im Ergebnis gleich B. Rudin/B. Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Rz. 56 zu § 7.

Bezüglich der Frage, ob im Empfängerstaat eine Gesetzgebung besteht, welche angemessenen Schutz gewährleistet, orientiert sich das kantonale Datenschutzrecht häufig daran, ob der Staat des Empfängers die Europarats-Konvention 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten beigetreten ist[36]. Orientierung bietet die vom Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (EDÖB) geführte Staatenliste[37], aus welcher entnommen werden kann, ob in der Beurteilung des EDÖB ein Staat über ein angemessenes Datenschutzniveau verfügt.[38] Als Länder mit angemessenem Datenschutz gelten insbesondere die Mitgliedstaaten der EU und des EWR.

Über keinen angemessenen gesetzlichen Datenschutz verfügen insbesondere die USA. Mit dem Swiss – US Privacy Shield Abkommen[39], welches im Januar 2017 zwischen der Schweiz und den USA vereinbart wurde, verfügen jedoch US Unternehmen seit dem 12.4.2017 über die Möglichkeit, sich beim US Department of Commerce zertifizieren zu lassen, womit sie aus schweizerischer Sicht gleich behandelt werden dürfen wie ein Datenempfänger, welcher sich in einem Staat mit einem angemessenen Datenschutzniveau befindet.

Fehlt auf Seiten des Empfängers ein angemessenes Datenschutzniveau , so ist eine grenzüberschreitende Datenbekanntgabe nur unter besonderen Bedingungen zulässig. In der Praxis von besonderer Bedeutung ist in diesem Zusammenhang die Vereinbarung von hinreichenden vertraglichen Garantien.

Beispiele:
Kanton Bern:
Art. 14a Abs. 2 KDSG
[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,
b die betroffene Person im Einzelfall eingewilligt hat,
c die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt,
d die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist,
e die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen oder
f die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

Kanton Luzern
Art. 11a Abs. 2 DSG
[2] Fehlt eine 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,
b die betroffene Person im Einzelfall eingewilligt hat,
c die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt,
d die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist,
e die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen,
f die betroffene Person die Daten allgemein zugänglich gemacht hat und eine Bearbeitung nicht ausdrücklich untersagt hat.

Kanton Zürich

[36] So der Kanton Zürich gemäss § 19 IDG, der Kanton Basel-Stadt gemäss § 23 IDG oder der Kanton Thurgau gemäss §9a DSG.

[37] Publiziert unter https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html

[38] So verweist z.B. die IDV des Kantons Zürich in § 22 ausdrücklich auf diese Liste.

[39] Zum Swiss – US Privacy Shield Abkommen vgl. die Informationen unter https://www.edoeb.admin.ch/datenschutz/00626/00753/01405/index.html?lang=de

§ 19 IDG
An Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen, gibt das öffentliche Organ Personendaten bekannt, wenn
a. im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist,
b. eine gesetzliche Grundlage dies erlaubt, um bestimmte Interessen der betroffenen Person oder überwiegende öffentliche Interessen zu schützen, oder
c. vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen werden.

In anderen Kantonen[40] wird für die Voraussetzungen bezüglich der Weitergabe von Personendaten in Länder ohne angemessenen gesetzlichen Datenschutz auf das Zusatzprotokoll zur Europarats-Konvention 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten verwiesen. Dieses Protokoll sieht in Art. 2 Abs. 2 lit. b insbesondere auch die Möglichkeit vor, durch vertragliche Regelungen mit dem Datenempfänger ein angemessenes Datenschutzniveau sicherzustellen.

Für entsprechende vertragliche Vereinbarungen empfiehlt es sich, entsprechend Musterklauseln zu verwenden, wie den Mustervertrag des Europarates oder die von der EU-Kommission veröffentlichten Standardvertragsklauseln[41].

Je nach Kanton bestehen jedoch auch Sonderbestimmungen, die im Fall der Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten ausschliessen, dass durch vertragliche Vereinbarungen ein angemessenes Datenschutzniveau geschaffen werden kann.

Beispiel:
Kanton Solothurn Ziff.5 AGB ISDS:
Serverstandort
Die Leistungserbringerin verpflichtet sich, die Informationen ausschliesslich auf Servern zu bearbeiten, die sich physisch in der Schweiz befinden oder in einem Staat, welcher dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Europarats-Konvention 108; SR 0.235.1) beigetreten ist.

6.2 Erhöhte Risiken

Mit der Weitergabe von Informationen bzw. Personendaten zur Bearbeitung im Ausland können, abhängig vom Land, in welchem die Datenverarbeitung stattfindet, erhöhte Risiken für die Wahrung des Datenschutzes verbunden sein. Bereits vor dem Abschluss eines Vertrages zur Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten kann es schwieriger sein zu überprüfen, ob ein ausländischer Anbieter auch geeignet ist, als dies im Vergleich bei inländischen Anbietern der Fall ist. Ebenso ist die Durchführung von Kontrollen bezüglich der Einhaltung der mit dem Auftragsbearbeiter getroffenen Vereinbarungen, je nach Land, in welchem die Datenbearbeitung stattfindet, wesentlich aufwändiger als im Inland.

Erhöhte rechtliche Risiken ergeben sich daraus, dass die allfällig notwendige gerichtliche Durchsetzung der mit dem Auftragsbearbeiter getroffenen vertraglichen Vereinbarungen im Ausland für ein öffentliches Organ aus der Schweiz schwieriger bzw. aufwändiger ist als im Inland. Das Gleiche gilt mit Bezug auf die strafrechtliche Verfolgung der Verletzung von gesetzlichen Geheimhaltungspflichten. Zudem besteht das Risiko, dass ausländische Behörden nach dem im betreffenden Staat geltenden Recht auf die Daten zugreifen können, welches allein mit vertraglichen Vereinbarungen mit dem Auftragsbearbeiter und dessen allfälligen Subunternehmern nicht beeinflusst werden kann.

Auch wenn im Vertrag mit einem ausländischen Auftragsbearbeiter schweizerisches Recht als anwendbar erklärt und ein Gerichtsstand in der Schweiz vereinbart wird, vermag dies die genannten Risiken nur

[40] So z.B. Art. 9a Abs. 2 DSG des Kantons Thurgau.

[41] Der Mustervertrag des Europarates sowie die EU-Standardvertragsklauseln sind am einfachsten auf der Website des EDÖB unter folgendem Link zu finden: https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html.

beschränkt zu vermindern, denn auch wenn gegen den Auftragsbearbeiter in der Schweiz geklagt werden kann und auf den Vertrag schweizerisches Recht anwendbar ist, so muss das Urteil im Ausland vollstreckt werden.

Es besteht daher allgemein die Auffassung, dass bei der Auslagerung der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen Zurückhaltung geübt werden sollte, oder es wird empfohlen, sogar generell auf die Auslagerung solcher Daten ins Ausland zu verzichten.

Aus diesen Gründen bedarf die Auslagerung einer Datenbearbeitung ins Ausland in den genannten Fällen (besonders schützenswerte Personendaten, Persönlichkeitsprofile, der Geheimhaltung unterliegende Daten) jedenfalls eine besondere Rechtfertigung. Diese Rechtfertigung kann darin liegen, dass die Daten durch Anonymisierung oder Pseudonymisierung vor der Weitergabe ins Ausland entpersonalisiert werden oder dass die unbefugte Kenntnisnahme durch Personen im Ausland durch technische Verschlüsselung oder andere technische Massnahmen, z.B. durch Einrichtung eines Trusted Execution Environment (TEE)[42], verhindert wird.

7. Geheimhaltungsvorschriften

Auch wenn die Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten nach den Bestimmungen des kantonalen Datenschutzrechts sowie der Regelungen betreffend den Einsatz von Informatikmitteln und die Informationssicherheit zulässig ist, muss jeweils speziell geprüft werden, ob nicht Geheimhaltungsvorschriften entgegenstehen.

Im Vordergrund steht hier das Amtsgeheimnis.

7.1 Allgemeines Amtsgeheimnis – Art. 320 Strafgesetzbuch

Unter das Amtsgeheimnis fallen alle Tatsachen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung der Geheimnisherr ein berechtigtes Interesse hat. Geheimnisherr können dabei sowohl der Staat bzw. das öffentliche Organ als auch Private sein, die dem Staat bzw. einem öffentlichen Organ Informationen über sich liefern bzw. über welche Informationen beschafft werden.

Das Amtsgeheimnis gilt für Mitglieder von Behörden und Beamte. Als Beamte gelten dabei alle Personen, die eine amtliche Aufgabe erfüllen oder an deren Erfüllung beteiligt sind, unabhängig davon, ob sie in einer formellen Beamtenstellung stehen, privatrechtlich angestellt sind oder allenfalls auch nur im Rahmen eines Auftragsverhältnisses handeln[43]. Die Verletzung des Amtsgeheimnisses kann auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bis maximal 180 Tagessätze à CHF 3'000.- bestraft werden.

Es wird allgemein davon ausgegangen, dass das allgemeine Amtsgeheimnis als solches einer Auslagerung der Datenbearbeitung nicht entgegensteht. Andernfalls wären Bestimmungen des kantonalen Rechts, welche die Möglichkeit der Auslagerung der Datenbearbeitung an externe Dritte vorsehen[44], praktisch gegenstandslos.

Wenn dem Amtsgeheimnis unterstehende Daten zur Bearbeitung an einen Dritten ausgelagert werden, untersteht dieser durch die Auftragserteilung mit Bezug auf die an ihn ausgelagerte Tätigkeit ebenfalls dem Amtsgeheimnis. Durch entsprechende vertragliche Regelungen ist zudem sicherzustellen, dass der Dritte sich bewusst zur Geheimhaltung verpflichtet.

---

[42] Siehe vorne Fussnote 1.

[43] Sogenannter funktioneller Beamtenbegriff.

[44] Vgl. die Beispiele oben in Ziff. 5.1.

7.2 Weitere Geheimhaltungspflichten

Wie bereits erwähnt[45], bestehen neben dem Amtsgeheimnis noch eine ganze Reihe von besonderen Geheimhaltungsvorschriften. Bei diesen ist jeweils gesondert zu prüfen, ob und, falls ja, unter welchen Voraussetzungen sie eine Weitergabe von der Geheimhaltung unterliegenden Daten an externe Auftragsbearbeiter zulassen.

So steht z.B. die Geheimhaltungspflicht gemäss Art. 33 ATSG, welche auch für kantonale öffentliche Organe gilt, soweit sie an der Durchführung des Sozialversicherungsgesetzes des Bundes beteiligt sind, einer Auslagerung nicht entgegen, denn in den einzelnen Sozialversicherungsgesetzen ist ausdrücklich vorgesehen, dass die Durchführungsorgane Personendaten von Dritten bearbeiten lassen dürfen.[46]

7.3 Weitergabe von geheimen Daten ins Ausland

Falls sich der Auftragnehmer, an welche Informatikleistungen bzw. die Bearbeitung geheimer Daten ausgelagert werden sollen, im Ausland befindet, ist besondere Vorsicht geboten. Gegenüber Personen im Ausland ist die Durchsetzung von allfälligen strafrechtlichen Sanktionen im Fall von Geheimnisverletzungen nicht in gleicher Weise sichergestellt wie gegenüber Personen, die in der Schweiz[47] handeln. Auch besteht die Möglichkeit, dass ausländische Behörden unter bestimmten Voraussetzungen auf Daten zugreifen können, welche nicht denjenigen des schweizerischen Rechts entsprechen.

Aus der mangelnden Durchsetzbarkeit des schweizerischen Strafrechts im Ausland wird der Schluss gezogen, dass die Weitergabe von der Geheimhaltung unterliegenden Daten nur mit zusätzlichen Sicherheitsmassnahmen zulässig ist, welche die Kenntnisnahme der geheimen Informationen durch Personen im Ausland verhindern. Es gilt das oben[48] zur Weitergabe von besonders schützenswerten Personendaten und Persönlichkeitsprofilen ins Ausland Gesagte entsprechend.

8. Informations-, Prüf- und Bewilligungsverfahren

Es ist jeweils zu prüfen, ob das kantonale Recht für die Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten ein Prüf- bzw. Genehmigungsverfahren vorsieht. Die Anknüpfungskriterien für solche Verfahren sind dabei im kantonalen Recht unterschiedlich. Teilweise wird generell an die Auslagerung von Informatikleistungen angeknüpft, während in anderen Kantonen an die Art der betroffenen Daten (besonders schützenswerte Personendaten/Persönlichkeitsprofile, der Geheimhaltung unterliegende Daten) oder die mit der Datenbearbeitung verbundenen Risiken angeknüpft wird. Häufig ist eine Genehmigungs- oder Informationspflicht vorgesehen, wenn bei der Weitergabe von Personendaten ins Ausland der Datenschutz durch besondere vertragliche Garantien gewährleistet wird.[49]

Beispiele:
1. Anknüpfung an die Auslagerung von Informatikleistungen:

- **Kanton Thurgau**: Gemäss § 9 des Reglementes des Regierungsrates über den Einsatz der Informatik ist die Verwendung von fremder Hard- und Software, d.h. Hard- und Software, an welcher dem Kanton keine Eigentums- oder Nutzungsrechte zustehen, nur mit der Bewilligung des Amtes für Informatik zulässig.

[45] Oben Ziff. 3.3

[46] Vgl. AHVG Art. 49a, IVG Art. 66 i.Vrb. mit Art. 49a AHVG, KVG Art. 84, UVG Art. 96.

[47] Vgl. R. Bühler/C. Rampini, Rz. 15 zu Art. 10a, in: Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, Basel, 3. Aufl., 2014 SK DSG- Rz. 15.

[48] Ziff. 7.2.

[49] Vgl. dazu oben Ziff. 7.1.

- **Kanton Luzern**: Gemäss § 14 des Informatikgesetzes des Kantons Luzern ist die Auslagerung von Informatikleistungen von übergeordnetem oder strategischem Interesse der Genehmigung des Regierungsrates unterstellt. Sonstige Auslagerungen unterliegen der Meldepflicht an die zuständige Behörde.

Nach § 61a der Verordnung zum Personalgesetz bedarf die Auslagerung von Informatikleistungen, welche das Personalinformationssystem betreffen, der Genehmigung des Regierungsrates.

2. Anknüpfung an die Art der bearbeiteten Daten bzw. die Risiken der Datenbearbeitung:

- **Kanton Bern § 17a KDSG**:
  Vorabkontrolle
  Beabsichtigt eine Behörde, Personendaten einer grösseren Anzahl von Personen elektronisch zu bearbeiten, unterbreitet sie die beabsichtigte Datenbearbeitung vor deren Beginn der Aufsichtsstelle zur Stellungnahme, wenn
  a zweifelhaft ist, ob eine genügende Rechtsgrundlage besteht,
  b besonders schützenswerte Personendaten bearbeitet werden,
  c eine besondere Geheimhaltungspflicht besteht oder
  d technische Mittel mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen eingesetzt werden.

- **Kanton Zürich § 17a IDG:**
  Vorabkontrolle
  Das öffentliche Organ unterbreitet eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung.

3. Informations-/Genehmigunspflicht von besonderen vertraglichen Garantien zur Gewährleistung des Datenschutzes im Ausland

- **Kanton Bern**: Art. 14a Abs. 2 lit. a und Abs. 3 KDSG: Informationspflicht
- **Kanton Wallis**: Art. 25 Abs. 2 lit. a und Abs. 3 GIDA: Genehmigungspflicht

Für Ihren Auftrag bedanken wir uns und ich stehe Ihnen gerne für allfällige Rückfragen und weitere Informationen zur Verfügung.

Mit freundlichen Grüssen

Dr. U. Widmer, Rechtsanwältin

Anhang zum Gutachten vom 31. Januar 2018

Checkliste Version 1.0 für kantonale und kommunale Auftraggeber betreffend rechtliche Rahmenbedingungen für die Nutzung von Cloud-Services[1]

1. Welche Arten von Daten sind betroffen?

1.1 Sachdaten?

1.2 Personendaten?

1.2.1 einfache Personendaten (alle Daten mit einem Bezug zu einer bestimmten oder bestimmbaren Person)

1.2.2 besonders schützenswerte Personendaten[2]

1.2.3 Persönlichkeitsprofile

1.3 Geheime Daten?

1.3.1 Amtsgeheimnis (Art. 320 StGB)

1.3.2 Berufsgeheimnis (Art. 321 StGB)

1.3.3 Steuergeheimnis

1.3.4 andere

2. Cloud-Anbieter

2.1 Wo werden die Daten gespeichert (Standorte Server bzw. Rechenzentren)?

2.1.1 in der Schweiz

2.1.2 im Raum EU/EWR

2.1.3 in sonstigen Ländern

2.2 Werden Daten auch an anderen Orten als den Speicherorten bearbeitet bzw. erfolgen von anderen Orten Zugriffe auf die gespeicherten Daten?

2.2.1 in der Schweiz

2.2.2 im Raum EU/EWR

2.2.3 in sonstigen Ländern

3. Datenbearbeitung durch Dritte

3.1 Vertrag mit dem Anbieter[3]

Falls Personendaten betroffen sind, ist im Vertrag mit dem Anbieter die Auftragsdatenbearbeitung zu regeln, d.h. es ist sicherzustellen, dass

3.1.1 die Datenbearbeitung durch den Anbieter (und seine ev. Subunternehmer) nur im Umfang und zu denjenigen Zwecken, wie dies für den Auftraggeber selbst zulässig ist, erfolgt;

3.1.2 der Anbieter (und seine ev. Subunternehmer) verpflichtet sind, angemessene organisatorische und technische Schutzmassnahmen zur Wahrung der Datensicherheit zu ergreifen;

---

[1] Die vorliegende Checkliste vermittelt eine strukturierte Übersicht über diejenigen Punkte, die aus rechtlicher Sicht im Zusammenhang mit einem Cloud Projekt für ein öffentliches Organ im Allgemeinen zu berücksichtigen sind. Die Checkliste ist jedoch aufgrund der Unterschiede in den verschiedenen kantonalen Rechtsordnungen nicht abschliessend. Sie kann damit als Basis bzw. als Hilfestellung für die Erarbeitung eigener Checklisten durch die Verantwortlichen in den einzelnen Kantonen dienen, welche auf die jeweiligen spezifischen Gegebenheiten im betreffenden Kanton abgestimmt sind.

[2] Besonders schützenswerte Personendaten sind Angaben über
a. die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit;
b. den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand;
c. Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung;
d. polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen.
Zitat aus Art. 3 DSG Kt. BE. Die Umschreibung in den kantonalen Datenschutzgesetzen ist weitgehend identisch mit derjenigen des Kt. Bern.

[3] Eine Liste der wesentlichen Vertragspunkte findet sich in Kap. 5.2.1 des Gutachtens für die SIK von Frau Dr. Widmer vom 31,1.2018 zum Thema „Klärung und Analyse der rechtlichen Grundlagen für die Integration von 'Platform-as-a-Service' und 'Software-as-a-Service' in der öffentlichen Verwaltung".

3.1.3 der Anbieter zur Information über die Datenbearbeitung (z.B. bei Datenschutzverletzungen) verpflichtet ist und Kontrollmöglichkeiten für den Auftraggeber bestehen (z.B. betreffend Subunternehmer, Serverstandorte, Einhaltung der Datensicherheit);

3.1.4 verschiedene Kantone (z.Bsp. BE, ZH, SO) kennen besondere Allgemeine Geschäftsbedingungen zur Regelung des Datenschutzes und der Datensicherheit bei der Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten. Hier ist jeweils zu prüfen, ob solche AGB aufgrund ihres Geltungsbereichs[4] auf ein bestimmtes Projekt Anwendung finden, und falls ja, sind sie als Bestandteil des Vertrages mit dem Anbieter zu erklären.

3.2 Datensicherheit

3.2.1 Es ist zu prüfen, ob die Sicherheitsmassnahmen des Anbieters den allgemeinen Anforderungen gemäss kantonalem Recht entsprechen.

3.2.2 Es ist zu prüfen, ob für die Informatikauslagerung besondere kantonale Anforderungen zur Datensicherheit bestehen, und ob diese vom Cloud Services Anbieter erfüllt werden. Entsprechende kantonale Regelungen finden sich, je nach Kanton, neben den gesetzlichen Bestimmungen zum Datenschutz und zur Informatik auch in Allgemeinen Geschäftsbedingungen, die jeweils als Bestandteil des Vertrages mit dem Cloud Services Anbieter zu vereinbaren sind.

4. Weitergabe der Daten ins Ausland

4.1 Bei Speicherorten für die Daten ausserhalb des EU/EWR-Raumes[5] oder bei Zugriff auf die Daten von ausserhalb dieses Raumes sind besondere vertragliche Garantien für einen angemessenen Datenschutz erforderlich, z.B. durch:

4.1.1 Standardklauseln der EU-Kommission

4.1.2 Mustervertrag des Europarates

4.2 Für die Bearbeitung von Personendaten in den USA kann der angemessene Datenschutz auch durch Zertifizierung des Cloud Services Anbieters (bzw. des betreffenden Subunternehmers) gemäss dem Swiss-US Privacy Shield erreicht werden.

4.3 Die Datenweitergabe ins Ausland ist mit einem erhöhten Risikopotential verbunden (erschwerte Kontrolle und Durchsetzung der Vertragspflichten gegenüber dem Anbieter sowie Risiko des Zugriffs ausländischer Behörden), daher sind bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen zusätzliche Schutzmassnahmen zu treffen:

- Pseudonymisierung (soweit praktikabel)
- Anonymisierung (sofern vom Nutzungszweck her möglich)
- genügend starke Verschlüsselung der Daten bei Transfer und Speicherung mit Schlüsselverwaltung durch den Auftraggeber in der Schweiz
- Nutzung weiterer Sicherheitsfeatures, z.B. Trusted Execution Environment für die Bearbeitung der Daten in der Cloud bzw. dem Zugriff zu Wartungszwecken durch den Cloud Services Anbieter.

5. Geheimhaltungspflichten

5.1 Die Weitergabe von Daten an Cloud Services Anbieter bzw. Auftragsdatenbearbeiter ist nur zulässig, wenn keine Geheimhaltungspflicht dies verbietet.

5.2 Wegen der erschwerten Durchsetzung des schweizerischen Strafrechts gegenüber Personen im Ausland und der daraus resultierenden Abschwächung des Geheimnisschutzes sind daher bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen zusätzliche Schutzmassnahmen zu treffen:

- Pseudonymisierung (soweit praktikabel);
- Anonymisierung (sofern vom Nutzungszweck her möglich)

---

[4] Dieser ist jeweils nicht einheitlich definiert und erfasst z.T. alle öffentlichen Organe, teilweise nur solche der zentralen kantonalen Verwaltung oder es sind vom allgemeinen Geltungsbereich spezielle Ausnahmen definiert.

[5] Ausserhalb des EU/EWR-Raumes verfügen gemäss der Staatenliste des EDÖB nur wenige Staaten über einen gleichwertigen Datenschutz (Kanada, Argentinien, Uruguay, Israel, Neuseeland und unter bestimmten Bedingungen Australien), bei denen auf besondere vertragliche Garantien verzichtet werden kann.

- genügend starke Verschlüsselung der Daten bei Transfer und Speicherung mit Schlüsselverwaltung durch den Auftraggeber in der Schweiz
- Nutzung weiterer Sicherheitsfeatures, z.B. Trusted Execution Environment für die Bearbeitung der Daten in der Cloud.

6. Genehmigungs- und Prüfverfahren

6.1 Es ist zu prüfen, ob bereits die Auslagerung von Informatikleistungen als solche nach kantonalem Recht einer Genehmigung bedarf.

6.2 Bei Projekten, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile betreffen oder erhöhte Risiken für die betroffenen Personen beinhalten, ist zu prüfen, ob vom kantonalen Recht eine sogenannte Vorabkontrolle durch die Datenschutzaufsichtsstelle verlangt wird.

6.3 Werden Daten in ein Land ohne hinreichenden gesetzlichen Datenschutz weitergegeben und der Datenschutz daher durch vertragliche Garantien mit dem Datenempfänge gewährleistet, so ist zu prüfen, ob das kantonale Recht die Meldung der Vertragsgarantien an die Datenaufsichtsstelle oder die Genehmigung durch diese verlangt.
