privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Merkblatt Cloud-spezifische Risiken und Massnahmen

1 Einleitung

Öffentliche Organe nehmen für ihre Datenbearbeitungen in vielfältiger Art und Weise die Dienstleistungen Dritter in Anspruch. Für die Auslagerung von Datenbearbeitungen an Dritte enthalten die (Informations- und) Datenschutzgesetze regelmässig Bestimmungen, die im Wesentlichen festhalten, dass das öffentliche Organ:

- Datenbearbeitungen auslagern darf, wenn und soweit im konkreten Kontext nicht gesetzliche Geheimhaltungsvorschriften (wie z.B. Amtsgeheimnis nach Art. 320 StGB, besondere Geheimhaltungspflichten oder Berufsgeheimnisse) oder vertragliche Vereinbarungen entgegenstehen,

- sicherstellen muss, dass die Dritten die (Personen-)Daten nur so bearbeiten, wie dies das öffentliche Organ selbst auch tun dürfte,

- sich insbesondere vergewissern muss, dass die Dritten in der Lage sind, die Informationssicherheit zu gewährleisten, und

- auch bei einer Auslagerung für die Datenbearbeitung vollumfänglich verantwortlich bleibt.

Wie diese Verantwortung bei solchen **Auftragsdatenbearbeitungen** wahrzunehmen ist, haben verschiedene Datenschutzbehörden in Leitfäden und Checklisten festgehalten[1].

Die von Dritten zur Verfügung gestellten Datenbearbeitungsdienstleistungen basieren heute immer mehr auf der Verwendung von **Cloud-Technologie**[2] und ähnlichen Angeboten mit erhöhtem Risiko[3] für den Datenschutz.

Privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, will mit diesem Merkblatt aufzeigen, welche Risiken bei Cloud- und ähnlichen Dienstleistungen **zusätzlich zu denen einer herkömmlichen Auftragsdatenbearbeitung** hinzukommen oder sich akzentuieren und wie die Verantwortung diesbezüglich von den öffentlichen Organen konkret

---

1 Vgl. die Links im Anhang.

2 Siehe dazu etwa die Definition von «Cloud Computing» des National Institute of Standards and Technology (NIST) unter <https://csrc.nist.gov/publications/detail/sp/800-145/final>.

3 Damit sind Leistungsangebote gemeint, welche nicht alle Merkmale einer bestimmten Definition von Cloud Computing aufweisen, aber mit den gleichen Risiken verbunden sind.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, 3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

wahrgenommen werden kann. Der Einfachheit halber ist nachfolgend nur von Cloud-Leistungen die Rede, die Ausführungen gelten aber für alle Auftragsdatenbearbeitungen mit erhöhtem Risiko.

Das Merkblatt legt den Fokus auf datenschutzrechtliche Risiken. Die öffentlichen Organe müssen andere Risiken für ihre Aufgabenerfüllung – z.B. bei der Durchsetzung von Vertragsbestimmungen oder bezüglich Datensouveränität – selbst mitberücksichtigen.

2 Bereiche mit erhöhten Risiken bei Datenbearbeitungen in der Cloud

Bei der Inanspruchnahme von Cloud-Lösungen von Drittanbietern bestehen oder akzentuieren sich Risiken in verschiedenen Bereichen. Das verantwortliche öffentliche Organ hat diese Risiken durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren; ist dies nicht möglich, so ist auf die Cloud-Leistung zu verzichten. Bei der Risikoanalyse für die konkrete Datenbearbeitung sind die cloud-spezifischen Risiken zu berücksichtigen und entsprechende Vorkehrungen zu treffen.

Im Vordergrund stehen fünf Risikobereiche:

- Vertragsgestaltung (nachfolgend Ziff. 2.1),
- Orte der Datenbearbeitungen einschliesslich ausländische Behördenzugriffe (Ziff. 2.2),
- Vertraulichkeit/Geheimnisschutz, Verschlüsselung und Schlüsselmanagement (Ziff. 2.3),
- Daten über die Nutzerinnen und Nutzer der Cloud-Dienste (Ziff. 2.4) und
- Unterauftragsverhältnisse (Ziff. 2.5).

Das cloud-spezifische Risiko wird primär von diesen fünf Risiken bestimmt.

Hinzu kommen weitere Risiken, die durch die Verwendung von Cloud-Infrastruktur mindestens akzentuiert werden: Meldepflichten (Ziff. 2.6), Kontrollrecht und -möglichkeit (Ziff. 2.7), Informationssicherheitsmassnahmen (Ziff. 2.8) und Pflichten bei Vertragsauflösung (Ziff. 2.9). Schliesslich ist auch zu berücksichtigen, dass sich die Abhängigkeiten vom Leistungserbringer (Verfügbarkeit, Migrationsaufwand bei Wechsel) weiter erhöhen.

2.1 Vertragsgestaltung

Das öffentliche Organ schliesst mit dem Cloud-Dienstleister einen schriftlichen Vertrag. Alternativ schliesst es sich einem Rahmenvertrag an oder akzeptiert die Allgemeinen Geschäftsbedingungen (AGB), welche die hier erwähnten Anforderungen erfüllen und nicht einseitig abänderbar sein dürfen.

Auf folgende drei Aspekte ist besonders zu achten:

- Die vertraglichen Verhaltens-/Sorgfaltspflichten des Anbieters sind vom öffentlichen Organ so auszugestalten, dass sie alle Anforderungen erfüllen, die das Organ nach dem

für es geltenden Datenschutzrecht selbst einhalten muss. Insbesondere darf der Anbieter nur *jene* Daten und diese nur *so* bearbeiten, wie es das Organ selbst tun dürfte[4].

Zudem muss der Anbieter bei der Erfüllung von datenschutzrechtlichen Ansprüchen der betroffenen Personen (Löschungs- respektive Berichtigungsansprüche) mitwirken.

- Das öffentliche Organ muss die Einhaltung der vertraglichen Pflichten kontrollieren können (vgl. unten Ziff. 2.7).

- Die Durchsetzung der vertraglichen Pflichten muss nach einer dem öffentlichen Organ vertrauten Rechtsordnung vor für das Organ einfach zugänglichen Gerichten möglich sein.

  Grundsätzlich muss daher auf das Vertragsverhältnis schweizerisches Recht anwendbar sein und für den Entscheid über Streitigkeiten aus dem Vertragsverhältnis ein Gerichtsstand in der Schweiz vereinbart werden.

  Die Anwendbarkeit des Rechts eines anderen Staates und ein ausländischer Gerichtsstand können in begründeten Fällen vereinbart werden, wenn sich daraus keine erhöhte Gefährdung der Grundrechte der betroffenen Personen ergibt, namentlich

  - wenn die Daten durch Verschlüsselung wirksam vor dem Zugriff durch Dritte (sowie den Anbieter der Cloud-Dienstleistung) geschützt werden können (Ziff. 2.3) oder

  - bei nicht sensitiven Daten[5], wenn das auf die Datenbearbeitung anwendbare Datenschutzrecht[6] über ein gleichwertiges Schutzniveau verfügt und dem Anbieter bei Verletzungen wirksame und abschreckende Sanktionen drohen (z.B. DSGVO der EU).

2.2 Orte der Datenbearbeitungen einschliesslich ausländische Behördenzugriffe

Der Anbieter muss offenlegen, in welchen Staaten er seine Cloud-Infrastruktur für die Bearbeitung von Personendaten (inkl. solche nach Ziff. 2.4) betreibt, damit die Zulässigkeit von Datenübermittlungen ins Ausland beurteilt und die Risiken in Bezug auf die Serverstandorte bei der Risikoabwägung mitberücksichtigt werden können.

- Datenbearbeitungsstandorte in der Schweiz sind zu bevorzugen (Sicherheit der Infrastruktur, z.B. in Bezug auf die Schutzziele Verfügbarkeit und Integrität, Zurechenbarkeit und Nachvollziehbarkeit, sowie Zugänglichkeit für Kontrollen, vgl. Ziff. 2.7).

---

4 Verhältnismässigkeit (Datenminimierung, Aufbewahrungsdauer etc.) und Zweckbindung (der Anbieter darf Personendaten nicht für andere als dem öffentlichen Organ selbst erlaubte Zwecke bearbeiten); beides gilt auch für die Daten über die Nutzerinnen und Nutzer der Cloud-Dienste gemäss Ziff. 2.4.

5 In diesem Dokument dient der Begriff «sensitive Daten» als Oberbegriff für alle Personendaten mit einem erhöhten Schutzbedarf, d.h. besonders schützenwerte Personendaten, Persönlichkeitsprofile und Personendaten unter einer gesetzlichen Geheimhaltungspflicht.

6 Das anwendbare Datenschutzrecht kann von den Parteien nicht gewählt werden; es ergibt sich aus dem persönlichen, sachlichen und räumlichen Geltungsbereich des betreffenden Datenschutzrechts selbst.

- Datenbearbeitungen an ausländischen Standorten[7] sind nur in Staaten zulässig, die über ein gleichwertiges Datenschutzniveau verfügen[8] oder in denen ein angemessener Datenschutz vertraglich – namentlich durch anerkannte Standardvertragsklauseln – erreicht werden kann. Letzteres ist dann nicht der Fall, wenn im betreffenden Staat behördliche Zugriffe möglich sind, die den verfassungsmässigen Grundrechtsgarantien (Legalitätsprinzip, Verhältnismässigkeit, Rechte der betroffenen Personen, Zugang zu unabhängigen Gerichten) nicht genügen. Diesfalls sind zusätzliche Massnahmen (insbesondere wirksame Verschlüsselung) zu treffen, damit die Übermittlung von Personendaten ins Ausland zulässig ist.

Achtung: Dem CLOUD Act[9] unterstehende Anbieter[10] müssen US-Behörden auch dann Zugriff auf gespeicherte Daten gewährleisten, wenn die Speicherung nicht in den USA, sondern z.B. in einem EU-Mitgliedstaat oder in der Schweiz erfolgt. Ein behördlicher Zugriff gestützt auf den CLOUD Act oder einen ähnlichen Rechtserlass eines anderen Staates wäre als unzulässige Bekanntgabe an Dritte zu beurteilen, weil sie ohne von der Schweiz anerkannte Rechtsgrundlage erfolgen würde. Das Risiko einer solchen Rechtsverletzung ist in der Analyse zu berücksichtigen und durch vertragliche Massnahmen (v.a. Verpflichtung des Cloud-Anbieters, alle Rechtsbehelfe zu ergreifen, um die Herausgabe der Daten zu verhindern, und das öffentliche Organ umgehend über behördliche Herausgabebegehren zu informieren, soweit dies dem Cloud-Anbieter erlaubt ist[11]) so weit als möglich zu reduzieren.

2.3 Vertraulichkeit/Geheimnisschutz, Verschlüsselung und Schlüsselmanagement

a. Alle Personendaten

Die vom Cloud-Anbieter bearbeiteten Personendaten (inkl. solche nach Ziff. 2.4) sind gegen unbefugte Zugriffe durch Dritte zu schützen. Unabhängig davon, ob es sich um «einfache» oder um sensitive Personendaten handelt, sind die Daten zumindest bei der Übertragung («data in transit») nach dem aktuellen Stand der Technik zu verschlüsseln.

Bei der Bearbeitung der Daten durch den Cloud-Anbieter ist die Vertraulichkeit durch geeignete Massnahmen angemessen zu schützen. Soweit dies durch eine Verschlüsselung erfolgt, ist zu beachten, dass verschlüsselt gespeicherte Daten («data at rest») während ihrer weiteren Bearbeitung («data in process») regelmässig nicht verschlüsselt bleiben[12].

---

7 Als Datenbearbeitung im Ausland ist auch der Zugriff auf in der Schweiz gespeicherte Daten von einem Standort im Ausland aus (z.B. für Supportleistungen) anzusehen, da dabei die Daten mindestens temporär ins Ausland übermittelt werden.

8 Vgl. die Länderliste des EDÖB unter <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html>.

9 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943, <https://www.congress.gov/bill/115th-congress/house-bill/4943>.

10 Vgl. zur Frage, wer dem CLOUD Act untersteht, das Whitepaper des US-Justizdepartements von April 2019, insb. S. 8: <https://www.justice.gov/opa/press-release/file/1153446/download>.

11 Soweit Behördenzugriffe ohne Information des verantwortlichen öffentlichen Organs erfolgen können, ist die Eintretenswahrscheinlichkeit nicht beurteilbar (weil nicht überprüfbar), so dass das Hauptaugenmerk auf dem Schadensausmass liegt, wo v.a. die Datenqualität massgeblich ist (sensitive Personendaten).

12 Dies gilt namentlich bei der Nutzung von Angeboten von Platform as a Service (PaaS) und Software as a Service (SaaS).

b. Besonders schützenswerte Personendaten

Bei besonders schützenswerten Personendaten ist dem Umstand, dass bei Cloud-Dienstleistungen regelmässig mehrere bzw. alle der hier erwähnten Risiken für die Vertraulichkeit bestehen, zusätzlich Rechnung zu tragen. Deshalb sind erhöhte Anforderungen an den Schutz der Vertraulichkeit der Daten zu stellen und in der Risikoabwägung zu berücksichtigen:

- Die Daten sind zu verschlüsseln und die Verschlüsselung hat durch das öffentliche Organ zu erfolgen. Die Schlüssel dürfen nur für das öffentliche Organ verfügbar sein. Sie sind vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen.

- Nur wenn sich daraus keine untragbaren Risiken für die Grundrechte der betroffenen Personen ergeben (was vom öffentlichen Organ nachvollziehbar darzulegen ist), kann eine Verschlüsselung beim Cloud-Anbieter geprüft werden. Hierbei muss die Ebene, auf welcher die Verschlüsselung erfolgt (Applikation, Datenbank oder Festplatte), berücksichtigt werden. Die Schlüssel können beim Cloud-Anbieter aufbewahrt werden, wenn dieser sich vertraglich verpflichtet, sie nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden. Zugriffe sind zu protokollieren. Ausserdem muss der Cloud-Anbieter die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden können.

c. Personendaten unter gesetzlicher Geheimhaltungspflicht

Personendaten, welche unter einer gesetzlichen Geheimhaltungspflicht stehen, dürfen dem Cloud-Anbieter (und gegebenenfalls dessen Subunternehmen) nur insoweit zugänglich gemacht werden, wie die betreffende Geheimhaltungsvorschrift den Beizug von Hilfspersonen erlaubt. Aus jener Vorschrift ist auch zu ermitteln, wer alles als Hilfsperson in Frage kommt und welche Anforderungen zu erfüllen sind, damit der Geheimnisschutz gewahrt bleibt. Die Verletzung von Geheimhaltungsvorschriften ohne anerkannten Rechtfertigungsgrund ist als rechtliche Schranke der Auslagerung und nicht nur als Risiko zu betrachten.

2.4 Daten über die Nutzerinnen und Nutzer der Cloud-Dienste

(Cloud-)Dienstleister bearbeiten in der Regel nicht nur die vom öffentlichen Organ innerhalb der Cloud-Dienste übermittelten Personendaten (insbesondere Inhaltsdaten), sondern auch von ihnen selbst bzw. ihren Diensten generierte Daten über die Nutzerinnen und Nutzer (z.B. Rand-, Telemetrie- oder Protokollierungsdaten). Diese zusätzlichen Personendaten sind mit der gleichen Sorgfalt zu behandeln wie die Daten, die das öffentliche Organ zur Aufgabenerfüllung bearbeitet. Sie müssen den gleichen vertraglichen Bestimmungen unterstellt sein und deren rechtmässige Bearbeitung und Schutz sind im gleichen Umfang sicherzustellen. Insbesondere müssen die Wahrung der Betroffenenrechte sowie die Vernichtung nach einer angemessenen bzw. gesetzlich vorgeschriebenen Aufbewahrungsfrist festgelegt sein und durch angemessene Massnahmen sichergestellt werden.

Diese zusätzlichen Personendaten dürfen ausschliesslich zu Zwecken aufgezeichnet und ausgewertet werden, welche auch dem öffentlichen Organ erlaubt wären, und diese sind dem Organ transparent offenzulegen. Dabei handelt es sich in aller Regel um nicht personenbezogene Zwecke. In Frage kommen etwa die Planung und das Reporting betreffend

technische Kapazitäten, die Aufrechterhaltung der Informations- und Dienstleistungssicherheit, die technische Wartung der Infrastruktur oder die Erfassung von nutzungsabhängigen Kosten. Bearbeitungen zu weitergehenden Zwecken sind nur mit anonym erhobenen oder vorgängig anonymisierten bzw. wirksam pseudonymisierten Daten zulässig.

Zu beachten ist, dass zusätzliche Personendaten je nach Kontext zu besonders schützenswerten Personendaten werden können (z.B. wenn Verbindungsdaten aufzeigen, dass sich eine betroffene Person in einer Psychiatrieanstalt oder Strafvollzugseinrichtung aufhält).

2.5 Unterauftragsverhältnisse (Subcontracting)

Das öffentliche Organ bleibt auch für Datenbearbeitungen verantwortlich, welche der Cloud-Anbieter seinerseits an Dritte (einschliesslich Mutter- und Tochterunternehmen) überträgt. Vor Vertragsabschluss zwischen dem öffentlichen Organ und dem Anbieter muss dieser deshalb seine Unterauftragsverhältnisse einzeln so offenlegen, dass das öffentliche Organ die Möglichkeit hat, die Zulässigkeit von Datenübermittlungen ins Ausland und die Risiken in Bezug auf die beteiligten Erbringer von Cloud-Dienstleistungen bei der Risikoabwägung beurteilen zu können. Im Vertrag ist festzuhalten, mit welchen Massnahmen der Cloud-Anbieter seine Subunternehmen instruiert und kontrolliert (inkl. Umgang mit Unter-Unterbeauftragten[ketten]).

Sub-Unternehmer aus Ländern mit nicht angemessenem Datenschutzniveau sollten ausgeschlossen werden; kann der ungenügende Datenschutz wegen möglicher Behördenzugriffe nicht vertraglich kompensiert werden, ist deren Beizug unzulässig.

Während der Vertragsdauer sind Änderungen in Unterauftragsverhältnissen dem öffentlichen Organ vorgängig anzuzeigen, mit der Möglichkeit der Kündigung des Vertragsverhältnisses.

2.6 Meldepflichten

Der Cloud-Dienstleister hat dem öffentlichen Organ Änderungen in der Art und Weise der Datenbearbeitung (insbesondere Datenbearbeitungsorte, Unterauftragsverhältnisse) sowie entsprechend dem anwendbaren Datenschutzrecht Sicherheitsvorfälle und getroffene Massnahmen zu deren Bewältigung zu melden, damit dieses seinerseits rechtzeitig Massnahmen in Bezug auf die Cloud-Dienstleistung treffen kann.

2.7 Kontrollrecht und -möglichkeit

Das öffentliche Organ hat sich ein Kontrollrecht vorzubehalten: Der Anbieter ist zu verpflichten, regelmässige Kontrollen seiner Cloud-Services nach anerkannten und dem Schutzbedarf entsprechenden Audit-Standards vorzunehmen. Die Prüfberichte sind dem öffentlichen Organ und der für dieses zuständigen Datenschutzaufsichtsbehörde auf Verlangen vorzulegen. Bei Bedarf (namentlich wenn die Kontrollen des Anbieters nicht alle Themen abdecken und sich z.B. auf Sicherheitsaspekte beschränken) müssen Prüfungen des Organs selbst bzw. seiner Aufsichtsbehörde oder durch diese beauftragte Dritte möglich sein.

2.8 Informationssicherheitsmassnahmen

Das öffentliche Organ hat sicherzustellen, dass ein dem Schutzbedarf entsprechender Schutz aller bearbeiteten Personendaten gewährleistet wird. Um das zu beurteilen, hat es

den Cloud-Dienstleister zu verpflichten, darzulegen, welche Schutzziele er mit welchen Informationssicherheitsmassnahmen erreicht.

Der Cloud-Dienstleister hat die Cloud-Services nach anerkannten, dem Schutzbedarf sowie dem Service entsprechenden Standards zu führen und weist dies gegebenenfalls mit geeigneten Zertifizierungen nach.

2.9 Pflichten bei Vertragsauflösung

Der Prozess bei der Auflösung des Vertragsverhältnisses ist bereits beim Vertragsabschluss festzuhalten (insbesondere Rücklieferung und Vernichtung der Daten).

3 Fazit

Öffentliche Organe können für ihre Datenbearbeitungen – wenn ihre Auslagerung nach den allgemeinen Regeln für die Auftragsdatenbearbeitung (siehe die Leitfäden im Anhang) zulässig ist – auch Cloud-Dienstleistungen Dritter in Anspruch nehmen. Dafür sind in einer umfassenden Risikoanalyse die spezifischen Risiken bei Inanspruchnahme von Cloud-Dienstleistungen zu berücksichtigen. Diese Risikoanalyse muss differenziert für die einzelnen Datenbearbeitungen die cloud-spezifischen Risiken sowie die entsprechenden Massnahmen aufzeigen, mit denen jene Risiken ausgeschlossen oder auf ein tragbares Mass reduziert werden können. Die Beurteilung soll aufzeigen, ob für die Datenbearbeitungen die Inanspruchnahme von Cloud-Diensten umfassend, teilweise oder nicht zulässig ist.

Grundsätzlich darf die Auslagerung von Datenbearbeitungen für die Grundrechte der betroffenen Personen nicht nachteilig sein. Damit die zusätzlichen Risiken aus der Nutzung von Cloud-Diensten dennoch als tragbar erscheinen können, ist von den öffentlichen Organen im Einzelfall darzulegen, durch welche unverzichtbaren Vorteile des Cloud-Dienstes gegenüber einer gleichwertigen Lösung *on premise* sowie gegenüber risikoärmeren Produkten anderer Anbieter die neuen Risiken aufgewogen werden.

Die öffentlichen Organe, die für ihre Aufgabenerfüllung Cloud-Dienstleistungen in Anspruch nehmen, tragen weiterhin vollumfänglich die Verantwortung für die Datenbearbeitung. Das öffentliche Organ (bzw. seine oberste Leitung[13]) ist angehalten, schriftlich zu bestätigen, dass es die Risiken verstanden hat und das Restrisiko übernimmt[14]. Die Übernahme von Restrisiken kann allenfalls auch Auswirkungen auf die Rechnungslegung haben, was durch die Finanzkontrollen zu prüfen ist. Den Exekutiven ist zu raten, die übernommenen (Rest-) Risiken regelmässig zu erfassen, da sie gegenüber Parlament und Volk letztlich die Verantwortung für den Schutz der Grundrechte der Bürgerinnen und Bürger und für das finanzielle Gebaren der Verwaltung zu tragen haben. Weil Cloud-Dienste stets weiterentwickelt werden und sich im Rahmen der Erneuerung der regelmässig befristeten Nutzungsverträge nicht verhandelbare Datenschutzbedingungen ändern können, ist von Anfang an im Auge

---

13 Im Hinblick auf die Einführung geeigneter Cloud-Dienste für eine gesamte Verwaltung ist als oberste Leitung die Regierung des betreffenden Gemeinwesens anzusehen.

14 Anders als im privaten Datenschutzrecht, wo Verantwortliche grundsätzlich jedes Risiko von Persönlichkeitsverletzungen übernehmen dürfen, können öffentliche Organe nicht nach freiem Ermessen beurteilen, ob ein Risiko für die Grundrechte der betroffenen Personen als tragbar erscheint und somit übernommen werden kann. Massgeblich sind vielmehr die verfassungsmässigen Vorgaben und dabei insbesondere das Verhältnismässigkeitsprinzip.

zu behalten, auf welche Ausstiegsszenarien das öffentliche Organ zurückgreifen kann, falls Veränderungen zu untragbaren Risiken führen.

Das öffentliche Organ muss seinerseits eine Datenschutz-Folgenabschätzung durchführen. Den zuständigen Datenschutzaufsichtsbehörden sind Risikoanalyse und Massnahmenplan nach Massgabe des anwendbaren Datenschutzrechts zur Prüfung vorzulegen (Vorabkontrolle bzw. Vorabkonsultation). Sie stehen den öffentlichen Organen auch beratend bezüglich rechtlicher, organisatorischer und technischer Fragen zur Seite.

Anhang: Leitfäden Auftragsdatenbearbeitung der kantonalen Datenschutzbeauftragten

Kanton Basel-Landschaft	Merkblatt Outsourcing
Kanton Basel-Stadt	Website «Handreichungen» Leitfaden Auftragsdatenbearbeitung
Kanton Genf	Fichier «Cloud Computing et protection des données personnelles au sein des institutions publiques genevoises»
Kanton St. Gallen	Merkblätter und Arbeitshilfen
Kanton Waadt	Check-list pour un contrat de sous-traitance de solution informatique
Kanton Zürich	Website «Auslagerung» Leitfaden Bearbeiten im Auftrag Leitfaden Auslagerung CLOUD-Act Leitfaden Verschlüsselung der Datenablage im Rahmen der Auslagerung Merkblatt Cloud Computing