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 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**:

> *Die Ressourcen für die Datenbearbeitungen werden dynamisch zur Verfügung gestellt und eine konkrete Lokalisation von Datenbearbeitungen und Daten ist nicht vorgesehen: Sie befinden sich eben in der «Cloud».*

Auch bei der Inanspruchnahme solcher Cloud-Dienstleistungen bleibt das öffentliche Organ vollumfänglich verantwortlich.

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

Somit ist vorerst nach den allgemeinen Datenschutzbestimmungen zu prüfen, ob eine Auslagerung überhaupt zulässig ist. Wenn dies der Fall ist und bei dieser Auftragsdatenbearbeitung Cloud-Infrastruktur genutzt werden soll, sind anschliessend die cloud-spezifischen Risiken zu prüfen.

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

[1] Vgl. die Links im Anhang 2.

privatim
c/o Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 205, CH-4010 Basel
Tel. +41 (61) 201 16 40
praesident@privatim.ch, www.privatim.ch

2 Akzentuierte oder zusätzliche Risiken bei Datenbearbeitungen in der Cloud

Bei der Inanspruchnahme von Cloud-Lösungen von Drittanbietern bestehen oder akzentuieren sich insbesondere die Risiken in folgenden Bereichen:

- Transparenz über die Standorte der Server;
- Kontrollmöglichkeiten (Abgrenzung der Datenbearbeitungen auf Cloud-Infrastruktur);
- Gestaltungsspielraum bei Standardangeboten (anwendbares Recht, Gerichtsstand, Serviceumfang, Sicherheitsmassnahmen, Vertragsinhalt generell);
- Durchsetzbarkeit von datenschutzrechtlichen Ansprüchen (Löschungs- respektive Berichtigungsansprüche);
- Vertraulichkeit (Verschlüsselung, Geheimnisschutz);
- Zugriffe von US-Behörden aufgrund des CLOUD Act[2] oder anderer ausländischer Behörden aufgrund ähnlicher Rechtserlasse[3];
- Transparenz über Informationssicherheitsmassnahmen (Datenverlust, -missbrauch);
- Transparenz über weitere Beteiligte (Unterauftragsverhältnisse, Wartung der Infrastruktur);
- Verfügbarkeit der Dienste und
- Transparenz bei Auflösung des Vertragsverhältnisses (Datenportabilität, Vernichtung der Daten).

3 Verantwortung des öffentlichen Organs bei der Inanspruchnahme von Cloud-Dienstleistungen

Das verantwortliche öffentliche Organ hat bei der Inanspruchnahme von Cloud-Dienstleistungen die spezifischen Risiken durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren. Bei der allgemeinen Risikoanalyse für die konkrete Datenbearbeitung sind die cloud-spezifischen Risiken zu berücksichtigen und entsprechende Vorkehrungen zu treffen.

Im Vordergrund stehen drei Risikobereiche:

- anwendbares Recht/Gerichtsstand (Ziff. 3.1),
- Ort der Datenbearbeitung (Serverstandorte) (Ziff. 3.2) und
- Geheimnisschutz/Schlüsselmanagement (Ziff. 3.3).

---

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

3 Im Folgenden unter CLOUD Act miterfasst.

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

Hinzu kommen weitere Risiken, die durch die Verwendung von Cloud-Infrastruktur mindestens akzentuiert werden (unten 3.4-3.10).

3.1 Anwendbares Recht, Gerichtsstand

Grundsätzlich soll auf das Vertragsverhältnis schweizerisches Recht (insbesondere das entsprechende Datenschutzgesetz) 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 kann vereinbart werden,

- wenn die Daten durch Verschlüsselung wirksam vor dem Zugriff durch Dritte (sowie den Anbieter der Cloud-Dienstleistung) geschützt werden können (Ziff. 3.3) oder
- bei nicht sensitiven Daten, wenn der entsprechende Staat über ein gleichwertiges Datenschutzniveau verfügt (z.B. EU-Mitgliedstaaten).

3.2 Ort der Datenbearbeitung

Der Anbieter muss offenlegen, wo er seine Cloud-Infrastruktur betreibt, damit 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).
- Bei ausländischen Standorten sind solche in Staaten, die über ein gleichwertiges Datenschutzniveau verfügen, vorzuziehen (Rechtssicherheit).

Dem CLOUD Act unterstehende Cloud-Anbieter[4] 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.

3.3 Geheimnisschutz, Verschlüsselung und Schlüsselmanagement

Daten (data at rest *und* data in transit) sind nach dem aktuellen Stand der Technik zu verschlüsseln.

Bei besonders schützenswerten Personendaten (inkl. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen) sind zusätzliche Anforderungen an die Verschlüsselung und das Schlüsselmanagement zu stellen und in der Risikoabwägung zu berücksichtigen:

---

[4] 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>.

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

- Ist dies nicht möglich, können die Schlüssel beim Cloud-Anbieter aufbewahrt werden, wenn er 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.

3.4 Vertrag

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.

3.5 Unterauftragsverhältnisse (Subcontracting)

Der Anbieter muss Unterauftragsverhältnisse offenlegen, damit die Risiken in Bezug auf die beteiligten Erbringer von Cloud-Dienstleistungen bei der Risikoabwägung mitberücksichtigt werden können.

3.6 Meldepflichten

Der Cloud-Dienstleister hat Änderungen in der Art und Weise der Datenbearbeitung (Standort, Unterauftragsverhältnisse) und Sicherheitsvorfälle dem öffentlichen Organ zu melden, damit rechtzeitig Massnahmen in Bezug auf die Cloud-Dienstleistung getroffen werden können.

3.7 Kontrollrecht und -möglichkeit

Das öffentliche Organ hat sich ein Kontrollrecht vorzubehalten: Der Anbieter ist zu verpflichten, regelmässige Kontrollen seiner Cloud-Infrastruktur nach internationalen Audit-Standards vorzunehmen und die Prüfberichte dem öffentlichen Organ und der für dieses zuständigen Datenschutzaufsichtsbehörde auf Verlangen vorzulegen.

3.8 Informationssicherheitsmassnahmen

Das öffentliche Organ hat sicherzustellen, dass ein dem Schutzbedarf entsprechender Schutz gewährleistet wird. Um das zu beurteilen, hat es den Cloud-Dienstleister zu verpflichten, in Bezug auf die Cloud-Infrastruktur darzulegen, welche Schutzziele er mit welchen Informationssicherheitsmassnahmen erreicht.

3.9 Betrieb der Cloud-Infrastruktur

Der Cloud-Dienstleister hat die Cloud-Infrastruktur nach internationalen Standards zu führen und weist dies allenfalls mit Zertifizierungen nach (ISO).

3.10 Pflichten bei Auflösung

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

4 Fazit

Öffentliche Organe können für ihre Datenbearbeitungen – wenn ihre Auslagerung nach den allgemeinen Regeln für die Auftragsdatenbearbeitung (siehe die Leitfäden im Anhang 2) 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 die cloud-spezifischen 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.

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 Leitung) ist anzuhalten, schriftlich zu bestätigen, dass es die Risiken verstanden hat und das Restrisiko übernimmt. 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.

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

Anhang 1: Beispiele für mögliche Gesamtbeurteilungen von Cloud-Risiken in Bezug auf anwendbares Recht/Gerichtsstand, Standort der Cloud-Infrastruktur und Geheimnisschutz/Verschlüsselung/Schlüsselmanagement

Fall	Anwendbares Recht / Gerichtsstand (3.1)	Standort der Cloud-Infrastruktur (3.2)	Schlüsselmanagement und Verschlüsselung (3.3)
1	Schweizerisches (Datenschutz-)Recht / Gerichtsstand in der Schweiz	(ausschliesslich) in der Schweiz	1a. beim öffentlichen Organ 1b. beim Cloud-Anbieter, der sich vertraglich verpflichtet, den Schlüssel nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden
	Beurteilung privatim:	*1a. Geringe cloud-spezifische Risiken* *1b. Erhöhte cloud-spezifische Risiken bei einem Anbieter, der dem CLOUD Act untersteht*	
	Empfehlung privatim:	*1a. Die Verwendung dieser Cloud-Lösung ist vom Ergebnis der Gesamtrisikobewertung der Auftragsdatenbearbeitung abhängig.* *1b. Die Risiken werden zusätzlich erhöht, wenn der Cloud-Anbieter dem CLOUD Act untersteht. Solche Cloud-Anbieter 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. Für das Bearbeiten von besonders schützenswerten Personendaten bzw. von Daten, die unter einem Berufs- oder besonderen Amtsgeheimnis stehen, ist auf die Verwendung einer solchen Cloud-Lösung zu verzichten. Das Risiko kann nur mit einer Verschlüsselung durch das öffentliche Organ (→Fall 1a) reduziert werden.*	
2	Schweizerisches (Datenschutz-)Recht / Gerichtsstand in der Schweiz	in einem (oder mehreren) ausländischen Staat(en) ohne gleichwertiges Datenschutzniveau	2a. beim öffentlichen Organ 2b. beim Cloud-Anbieter, der sich vertraglich verpflichtet, den Schlüssel nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden
	Beurteilung privatim:	*2a. Erhöhte cloud-spezifische Risiken* *2b. Hohe cloud-spezifische Risiken bei einem Anbieter, der dem CLOUD Act untersteht*	

	Empfehlung privatim:	*2a. Die Verwendung dieser Cloud-Lösung für das Bearbeiten von («gewöhnlichen») Personendaten ist möglich.* *Die Verwendung dieser Cloud-Lösung für das Bearbeiten von besonders schützenswerten Personendaten bzw. von Daten, die unter einem Berufs- oder besonderen Amtsgeheimnis stehen, ist jedoch mit erhöhten Risiken behaftet. Diese könnten verringert werden, wenn die Cloud-Infrastruktur sich in der Schweiz oder mindestens in einem Land mit einem gleichwertigen Datenschutzniveau befindet. Dies hat in die Gesamtbeurteilung der Risikoabwägung einzufliessen.* *2b. Dem CLOUD Act unterstehende Cloud-Anbieter müssen US-Behörden allerdings auch dann Zugriff auf gespeicherte Daten gewährleisten, wenn die Speicherung nicht in den USA erfolgt. Für das Bearbeiten von besonders schützenswerten Personendaten bzw. von Daten, die unter einem Berufs- oder besonderen Amtsgeheimnis stehen, ist auf die Verwendung einer solchen Cloud-Lösung zu verzichten. Das Risiko kann nur mit einer Verschlüsselung durch das öffentliche Organ (→ Fall 2a) reduziert werden.*	
3	Nicht schweizerisches (Datenschutz-)Recht / Gerichtsstand nicht in der Schweiz	in einem (oder mehreren) Staaten ohne gleichwertiges Datenschutzniveau	beim Cloud-Anbieter
	Beurteilung privatim:	*Sehr hohe cloud-spezifische Risiken*	
	Empfehlung privatim:	*Auf die Verwendung dieser Cloud-Lösung ist für das Bearbeiten von Personendaten zu verzichten.*	

Anhang 2: 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	Website «Informatik» Checkliste «Vereinbarungsinhalt beim Outsourcing»
Kanton Zürich	Website «Outsourcing» Leitfaden Bearbeiten im Auftrag Leitfaden Verschlüsselung der Datenablage im Rahmen der Auslagerung