KANTON AARGAU

Beauftragte für
Öffentlichkeit und
Datenschutz

Merkblatt

04.06.2019

(Stand
9.12.2019)

Auslagerung von Datenbearbeitungen: Besonderheiten des Cloud Computing

1. Einleitung

Öffentliche Organe nehmen für die Bearbeitung von Personendaten oft die Dienste Dritter in Anspruch. Dieses Merkblatt richtet sich an die öffentlichen Organe des Kantons Aargau, die Cloud Services von Drittanbietern nutzen oder nutzen wollen[1].

Bei der Auslagerung von Datenbearbeitungen bleibt das auslagernde öffentliche Organ für die Einhaltung des Datenschutzes verantwortlich. Die Inanspruchnahme von Cloud Services ist ein sogenanntes «Datenbearbeiten im Auftrag» (auch Auslagerung oder Outsourcing genannt) und muss den Ansprüchen an die Einhaltung des Datenschutzes ebenso genügen wie ein Outsourcing einer Datenbearbeitung im konventionellen Sinn. Da bei der Nutzung von Cloud Services die Risiken in Bezug auf die Verletzung der Persönlichkeitsrechte wesentlich höher sind als bei einem konventionellen Outsourcing, ist auf einzelne gesetzliche Anforderungen besonderes Augenmerk zu richten. Diese sind Gegenstand des vorliegenden Merkblatts. Die allgemeinen Anforderungen an das Datenbearbeiten im Auftrag sowie die Datensicherheit müssen weiterhin beachtet werden.

Ausgangspunkt der Nutzung von Cloud Services ist eine Risikoanalyse, welche die Anforderungen an den Cloud-Anbieter und im Weiteren den Inhalt des schriftlich zu vereinbarenden Vertrags massgeblich bestimmt. Die Cloud-spezifischen Punkte müssen detailliert geregelt und die Umsetzung der festgehaltenen Massnahmen regelmässig kontrolliert werden.

2. Cloud-Computing und Outsourcing

Die Inanspruchnahme von Cloud Services ist ein «Bearbeiten im Auftrag» gemäss § 18 IDAG (Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen[2]) und muss sich deshalb an diesen Voraussetzungen orientieren. Öffentliche Organe dürfen Cloud Services nutzen, wenn sie in der Lage sind, ihre in § 12a VIDAG (Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das

[1] Dieses Merkblatt wurde mit freundlicher Genehmigung des Datenschutzbeauftragten des Kantons Zürich basierend auf dessen Merkblatt «Cloud Computing» erstellt.
[2] SAR 150.700

Archivwesen[3]) umschriebenen Pflichten in Bezug auf Datenschutz und Informationssicherheit wahrzunehmen, denn sie bleiben weiterhin für die Datenbearbeitung verantwortlich (§ 18 Abs. 2 IDAG).

Die der Cloud eigenen Besonderheiten und die dadurch entstehenden Risiken, beispielsweise die Nutzung einer Infrastruktur durch mehrere Beteiligte, müssen durch angemessene Ausgleichsmassnahmen aufgefangen werden. Bei der Auswahl, der schriftlichen Vertragsgestaltung und der Umsetzung der Massnahmen müssen deshalb zusätzliche Punkte beachtet werden. Die grössten Herausforderungen bestehen in Bezug auf die Transparenz, die Kontrollen und allgemein in Bezug auf die Wahrnehmung der Verantwortung durch das öffentliche Organ.

3. Risikoanalyse und Anbieterauswahl

Vor der Auslagerung der Bearbeitung von Personendaten ist in aller Regel eine Datenschutz-Folgenabschätzung durchzuführen (vgl. Merkblatt IDAG und VIDAG – Was ist neu? Datenschutz-Folgenabschätzung [DSFA]). Dabei handelt es sich um einen schrittweisen Prozess: Die öffentlichen Organe führen für die auszulagernden Datenbearbeitungen eine Schutzbedarfsanalyse (§ 4 Abs. 2 VIDAG) durch. Je nach Gefährdungspotenzial erfolgt die Einstufung in eine der drei Sicherheitsstufen. Anschliessend werden die Schutzziele gemäss § 4 Abs. 1 VIDAG ermittelt (Inhalt der DSFA gemäss § 6a lit. a – c VIDAG). Aus diesen Beurteilungen resultieren die massgebenden Faktoren für die Auswahl des Cloud-Anbieters, denn sie bestimmen die grundlegenden organisatorischen, technischen und rechtlichen Anforderungen, die dieser zu erfüllen hat. Vom Cloud-Anbieter ist ein Nachweis über die technischen und organisatorischen Massnahmen sowie der rechtlichen Rahmenbedingungen zu verlangen, die zur Bewältigung der Risiken geplant sind (§ 6a lit. d VIDAG, ISDS-Konzept; dieser Nachweis kann im nächsten Schritt in die DSFA eingebaut bzw. dieser beilegt werden. Das Ergebnis der DSFA ist vom auslagernden Organ selbst festzustellen.)

Cloud-spezifische Risiken sind insbesondere bei den folgenden Punkten zu beachten:

- Wahrnehmung der Verantwortung durch beide Parteien
- Verlust der Kontrolle oder Verunmöglichen der Kontrollpflichten
- Durchsetzbarkeit der Löschungs- und Berichtigungsansprüche
- Gewährleistung eines gleichwertigen Datenschutzniveaus
- Umsetzung der notwendigen IT-Sicherheitsmassnahmen
- Überprüfbarkeit der Abläufe und Prozesse
- Nachvollziehbarkeit der Datenbearbeitungen
- Datenverlust
- Datenmissbrauch
- Eingeschränkte Verfügbarkeit der Dienste
- Portabilität und Interoperabilität

[3] SAR 150.711

Der Cloud-Anbieter hat über die rechtlichen, organisatorischen und technischen Rahmenbedingungen der angebotenen Dienstleistung zu informieren. Hilfsinstrumente können diesbezüglich Zertifikate oder unabhängige Auditberichte sein, die gewisse Aspekte der Dienstleistung transparent machen. Deren Aussagekraft hängt von der Berücksichtigung nationaler und internationaler Standards ab.

4. Vertragsgestaltung

Das öffentliche Organ muss seine Verantwortung für die Einhaltung des Datenschutzes (§ 18 Abs. 2 IDAG) auch in einer Cloud-Struktur wahrnehmen können. Den folgenden Punkten ist besondere Beachtung zu schenken

4.1 Kontrolle

Die Kontrollrechte des öffentlichen Organs sowie unabhängiger Aufsichtsbehörden (Datenschutzbeauftragter/Finanzkontrolle) in Bezug auf die ausgelagerte Tätigkeit sind zu verankern. Dies betrifft insbesondere auch die Kontrollmöglichkeit vor Ort (z. B. im Rechenzentrum). Ist dies nicht möglich, sind andere Kontrollmöglichkeiten vorzusehen, z.B. durch Einsicht auf Distanz oder durch vertragliche Verpflichtung des Cloud-Anbieters, regelmässig (z.B. alle zwei Jahre) Kontrollen nach internationalen Audit-Standards durchführen zu lassen. Der Cloud-Anbieter ist des Weiteren vertraglich zu verpflichten, die Prüfungsresultate unabhängiger Kontrollstellen dem öffentlichen Organ zur Verfügung zu stellen.

4.2 Rechte Betroffener

Die Gewährleistung des Auskunftsrechts von Personen über ihre gespeicherten Daten ist festzuhalten. Der Cloud-Anbieter hat die Durchsetzung der Rechte Betroffener auf Berichtigung und Löschung vertraglich zu garantieren und muss auch in der Lage sein, diese tatsächlich erfüllen zu können.

4.3 Ort der Datenbearbeitung

Es ist schriftlich zu vereinbaren, dass der Cloud-Anbieter über sämtliche möglichen Datenbearbeitungsorte Auskunft erteilen muss. Ortswechsel müssen gemeldet und vor dem Wechsel vom öffentlichen Organ bewilligt werden.

4.4 Gleichwertiges Datenschutzniveau

Datenbekanntgaben ins Ausland unterliegen den Bestimmungen von § 14 Abs. 3 und Abs. 4 IDAG. Diese gelten für die Inanspruchnahme von Cloud Services, wenn es sich um das Bearbeiten von Personendaten handelt. Sofern Cloud Services Datenbearbeitungen im Ausland beinhalten, dürfen diese nur ins Ausland ausgelagert werden, wenn ein der Schweiz gleichwertiges Datenschutzniveau besteht und/oder zusätzliche Sicherheitsmassnahmen umgesetzt werden. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte veröffentlicht eine Liste der Staaten mit angemessenem Datenschutzniveau[4].

[4] Staatenliste auf https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html

4.5 Unterauftragsverhältnisse

Unterauftragsverhältnisse müssen vor Vertragsabschluss offengelegt werden. Festzuhalten ist, dass nachträgliche Vereinbarungen nur mit Kenntnis und Zustimmung des öffentlichen Organs unterzeichnet werden dürfen (§ 18 IDAG). Diese Unter-Auftragnehmer müssen verpflichtet werden, Weisungen des Cloud-Anbieters zu beachten. Es ist sicherzustellen, dass sie sich auch an die vertraglich vereinbarten Verpflichtungen halten müssen.

4.6 Anwendbares Recht und Gerichtsstand

Grundsätzlich soll auf das Vertragsverhältnis schweizerisches Recht (insbesondere das IDAG) 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 Gerichts - stand können vereinbart werden,
- wenn die Daten durch Verschlüsselung wirksam vor Zugriffen geschützt werden können (vgl. Anhang) oder
- bei nicht sensitiven Daten, wenn der entsprechende Staat über ein gleichwertiges Datenschutzniveau verfügt (z.B. EU-Mitgliedstaaten).

4.7 Organisatorische und technische Sicherheitsmassnahmen

Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit müssen auch bei der Nutzung von Cloud Services gewährleistet sein. Die zu bearbeitenden Datenkategorien und deren Schutzbedarf sind vertraglich festzuhalten. Es ist zu vereinbaren, dass der Cloud-Anbieter das öffentliche Organ regelmässig über die Erfüllung der wichtigsten Massnahmen im IT-Sicherheitsbereich orientiert. Weiter muss der Cloud-Anbieter über sicherheitsrelevante Vorfälle orientieren.

Der Cloud-Anbieter muss die im Rahmen von § 4 VIDAG geforderten, nicht abschliessend aufgezählten technischen und organisatorischen Massnahmen garantieren. In einem Informationssicherheitskonzept hat er die organisatorischen und technischen Sicher- heitsmassnahmen wie kryptografische Verfahren, Identity- und Accessmanagement, Notfallmanagement usw. festzuhalten.

Speziell zu vereinbaren sind organisatorische und technische Massnahmen, die die Porta- bilität, die Interoperabilität sowie die Mandantentrennung gewährleisten.

4.8 Verschlüsselung von Personendaten bei Cloud Computing

Vgl. Übersicht Verschlüsselung von Personendaten bei Cloud Computing im Anhang.

5. Umsetzung der Massnahmen

Das öffentliche Organ muss die Umsetzung der organisatorischen, technischen und rechtlichen Rahmenbedingungen, wie im Vertrag festgehalten, regelmässig überprüfen.

6. Weiterer Hinweis: Cloud Computing im Schulbereich

Die Konferenz der Datenschutzbeauftragten Privatim hat ein Merkblatt Cloud Computing im Schulbereich herausgegeben.

Für Verwendung von Office 365 im Schulbereich kann auf den Leitfaden des Datenschutzbeauftragten des Kantons Zürich «office 365 im Bildungsbereich» abgestellt werden.

Anhang: Verschlüsselung von Personendaten bei Cloud Computing

<table>
<tr><th></th><th colspan="3">Personendaten unter Amtsgeheimnis</th><th colspan="2">Personendaten unter einer besonderen Schweigepflicht</th></tr>
<tr><td></td><td>Schweiz</td><td colspan="2">Ausland</td><td colspan="2">Schweiz/Ausland</td></tr>
<tr><td>Welche Daten erfordern eine Verschlüsselung?</td><td rowspan="2">Besonders schützenswerte Personendaten</td><td colspan="2">Gleichwertiges Schutzniveau?</td><td colspan="2" rowspan="2">Alle Personendaten</td></tr>
<tr><td></td><td>Wenn Ja: Bes. schütz. Personen-daten</td><td>Wenn Nein: Alle Personen-daten</td></tr>
<tr><td>Muss das Schlüsselmanagement beim öffentlichen Organ bleiben?</td><td colspan="2">Abhängig vom Ergebnis einer Risikobeurteilung[1]</td><td>Ja</td><td colspan="2">Ja</td></tr>
<tr><td>Gibt es Alternativen, wenn ein vollständiger Schlüsselverbleib beim öffentlichen Organ nicht möglich ist?</td><td colspan="2">Ja[2]</td><td>Nein</td><td colspan="2">Schweiz oder gleichwertiges Schutzniveau?</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Wenn Ja: Alternativen gegeben[2]</td><td>Wenn Nein: Auslage-rung un-zulässig</td></tr>
</table>

[1]Kriterien der Risikobeurteilung

- Anzahl betroffene Personen
- Komplexität der Infrastruktur
- Risiko und Schwere einer allfälligen Persönlichkeitsverletzung
- Ort der Datenbearbeitung
- Umfang der Kontrollen durch das verantwortliche öffentliche Organ
- Umfang der Sicherheitsmassnahmen durch das verantwortliche öffentliche Organ
- Aktuelle Risikolage

[2]Alternativen zur Verschlüsselung mit Schlüsselmanagement beim öffentlichen Organ

a) Vertragliche Absicherung
Der Auftragnehmer muss sich vertraglich verpflichten, den Schlüssel nur auf explizite Anfrage und nach expliziter Einwilligung des verantwortlichen öffentlichen Organs einzusetzen und auf die Daten zuzugreifen.

b) Unabdingbarkeit der Kenntnisnahme
Der Auftragnehmer darf Kenntnis der Daten erlangen, wenn dies für die Aufgabenerfüllung unabdingbar ist, beispielsweise bei der Wartung medizinischer Instrumente

c) Einwilligung der betroffenen Personen
Eine Auslagerung ist auch möglich, wenn die betroffenen Personen in die Offenlegung der von der besonderen Schweigepflicht (z.B. medizinisches Berufsgeheimnis) geschützten Daten einwilligen. Die Einwilligung hat informiert und freiwillig zu erfolgen.