privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Merkblatt

CLOUD COMPUTING

1 Einleitung

Dieses Merkblatt richtet sich an die öffentlichen Organe der Kantone und Gemeinden, welche Cloud-Services evaluieren oder solche bereits nutzen.

Die Inanspruchnahme von Cloud-Services ist ein «Bearbeiten im Auftrag» (auch Auslagerung oder Outsourcing genannt) und muss den Ansprüchen an die Informationsbearbeitung ebenso genügen wie ein Outsourcing einer Informationsbearbeitung im konventionellen Sinn. Da bei der Nutzung von Cloud-Services die Risiken in Bezug auf die Verletzung der Rahmenbedingungen und bei der Bearbeitung von Personendaten insbesondere in Bezug auf die Verletzung der Persönlichkeitsrechte wesentlich höher sind als bei einem konventionellen Outsourcing, ist auf einzelne, von den (Informations- und) Datenschutzgesetzen geforderten Bestimmungen spezielles Augenmerk zu richten.
Ausgangspunkt der Nutzung solcher 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 – (informations- und) datenschutzrechtlich betrachtet – ein «Bearbeiten im Auftrag» und muss sich deshalb an den entsprechenden Voraussetzungen der (Informations- und) Datenschutzgesetze orientieren. Öffentliche Organe dürfen Cloud-Services nutzen, wenn sie in der Lage sind, ihre Pflichten in Bezug auf Datenschutz und Informationssicherheit wahrzunehmen. Sie sind und bleiben für die Datenbearbeitung verantwortlich.

Die der Cloud eigenen Besonderheiten und der dadurch entstehenden Risiken, beispielsweise die Nutzung einer Infrastruktur durch mehrere Beteiligte, müssen durch angemessene Ausgleichsmassnahmen aufgefangen werden. Bei der Auswahl des Cloud-Anbieters und des Cloud-Angebotes, der schriftlichen Vertragsgestaltung und der Um-

privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati
c/o Datenschutzbeauftragter des Kantons Zürich
Postfach, CH-8090 Zürich
Tel. +41 (43) 259 39 99, Fax +41 (43) 259 51 38
geschaeftsstelle@privatim.ch, www.privatim.ch

setzung 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 Anbieter-Auswahl

Die öffentlichen Organe führen für ihre Informatiksysteme und –anwendungen eine Risikoanalyse durch. Dabei sind einerseits – abhängig vom Inhalt der Datenbearbeitung – die Schutzziele (bezüglich Vertraulichkeit, Verfügbarkeit und Integrität, evtl. auch Zurechenbarkeit und Nachvollziehbarkeit) zu bestimmen; andererseits ist das Gefährdungspotenzial zu ermitteln. Aus diesen Beurteilungen resultieren die massgebenden Faktoren für die Auswahl des Cloud-Anbieters und des Cloud-Angebotes, denn sie bestimmen die grundlegenden organisatorischen, technischen und rechtlichen Anforderungen, die der Anbieter zu erfüllen hat.

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

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

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 (informations- und) datenschutzrechtliche Verantwortung auch in einer Cloud-Struktur wahrnehmen können. Es ist deshalb detailliert und schriftlich in einem Vertrag festzuhalten, wer im Sinne der (Informations- und) Datenschutzgesetzgebung wofür verantwortlich zeichnet. Wenn für das Bearbeiten von Personendaten, insb. von besonders schützenswerten Personendaten oder Persönlichkeitsprofile eine Cloud-Lösung gewählt wird, dürfte es in aller Regel nicht ausreichen, Standard-AGBs eines allgemeinen Anbieters anzuerkennen.

4.1 Kontrolle

Die Kontrollrechte des öffentlichen Organs sowie unabhängiger Aufsichtsbehörden (Datenschutzbeauftragter, Finanzkontrolle) sind zu verankern. Dies betrifft insbesondere auch die Kontrollmöglichkeit vor Ort.
Weiter ist der Cloud-Anbieter zu verpflichten, regelmässig externe Kontrollen nach internationalen Audit-Standards durchführen zu lassen. Der Cloud-Anbieter ist zu verpflichten, die Prüfungsresultate unabhängiger Kontrollstellen dem öffentlichen Organ zur Verfügung zu stellen.

4.2 Rechte der betroffenen Personen

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.

4.3 Ort der Datenbearbeitung

In jedem Fall ist schriftlich zu vereinbaren, dass der Cloud-Anbieter über sämtliche möglichen Datenbearbeitungsorte Auskunft erteilen muss. Ortswechsel müssen gemeldet und vom öffentlichen Organ bewilligt werden.
Bei sensitiven Bearbeitungen (von besonderen Personendaten oder Persönlichkeitsprofilen, aber auch bei Daten, die einer besonderen gesetzlichen Geheimhaltungspflicht unterstehen oder aus anderen als aus Datenschutzüberlegungen als sensitiv beurteilt werden) ist zu dafür zu sorgen, dass ausländische Behörden nicht physisch auf die Daten greifen können (z.B. durch Beschlagnahme). In solchen Fällen ist vertraglich zu vereinbaren, dass alle Datenbearbeitungen ausschliesslich in der Schweiz stattfinden.

4.4 Gleichwertiges Datenschutzniveau

Datenbekanntgaben ins Ausland unterliegen regelmässigen spezifischen (informations- und) datenschutzgesetzlichen Bestimmungen. Die gleichen Überlegungen sind bei der Inanspruchnahme von Cloud-Services anzustellen, weil das öffentliche Organ verantwortlich bleibt. Wenn Cloud-Services das Bearbeiten von Personendaten beinhalten, dürfen diese Bearbeitungen nur ins Ausland ausgelagert werden, wenn ein der Schweiz gleichwertiges Datenschutzniveau besteht und/oder zusätzliche Sicherheitsmassnahmen um-

gesetzt werden.

4.5 Unterauftragsverhältnisse

Unterauftragsverhältnisse müssen vor Vertragsabschluss offen gelegt werden. Festzuhalten ist, dass nachträgliche Vereinbarungen nur mit Kenntnis und Zustimmung des öffentlichen Organs unterzeichnet werden dürfen. Diese «Unter-Auftragnehmer» müssen verpflichtet werden, Weisungen des Cloud-Anbieters zu beachten. Ausserdem sind bei sensitiven Bearbeitungen bezüglich Sitz des Unternehmens und Ort der Datenbearbeitung dieselben Anforderungen zu stellen wie beim Cloud-Anbieter.

4.6 Anwendbares Recht, Durchsetzung des Rechts

Ob schweizerisches Recht, insbesondere das kantonale das (Informations- und) Datenschutzgesetz anwendbar ist, hängt von der konkreten Regelung im Gesetz ab. Entscheidend bleibt, dass das öffentliche Organ, das verantwortlich bleibt, seine Verantwortung rechtlich und tatsächlich wahrnehmen kann. Haftungsausschlüsse in AGBs des Cloud-Anbieters können dem ebenso entgegenstehen wie ein Gerichtsstand oder Sitz des Cloud-Anbieters im Ausland. Es sollte nicht bloss ein Gerichtsstand in der Schweiz vereinbart werden, sondern bei sensitiven Datenbearbeitungen auch darauf geachtet werden, dass der Sitz des Cloud-Anbieters (wie auch der Ort der Datenbearbeitung: Ziffer 4.3) in der Schweiz liegt. Andernfalls muss das öffentliche Organ allenfalls schon ein Gerichtsurteil im Ausland erstreiten oder auch ein schweizerisches Gerichtsurteil im Ausland durchsetzen. Damit dürften öffentliche Organe regelmässig überfordert sein, womit die Durchsetzung in Frage gestellt ist und das öffentliche Organ seine Verantwortung nicht wahrnehmen kann.

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 IKT-Sicherheitsbereich orientiert. Weiter ist der Cloud-Anbieter zu verpflichten, über sicherheitsrelevante Vorfälle zu orientieren.
Der Cloud-Anbieter muss die im Rahmen der (informations- und) datenschutzgesetzlichen Informationssicherheitsbestimmungen geforderten, in der Regel nicht abschliessend aufgezählten Schutzziele garantieren. In einem Informationssicherheitskonzept hat er die organisatorischen und technischen Sicherheitsmassnahmen wie kryptografische Verfahren, Identity- und Accessmanagement, Notfallmanagement usw. festzuhalten. Beim Bearbeiten von besonderen Personendaten (besonders schützenswerte Personendaten und Persönlichkeitsprofile) hat er die organisatorischen und technischen Massnahmen in einem Managementsystem für Informationssicherheit zu verwalten.
Speziell zu vereinbaren sind organisatorische und technische Massnahmen, die die Portabilität, die Interoperabilität sowie die Mandantentrennung gewährleisten.

5 Umsetzung der Massnahmen

Die Umsetzung der organisatorischen, technischen und rechtlichen Rahmenbedingungen, wie im Vertrag festgehalten, muss durch das öffentliche Organ laufend überprüft werden.

6 Quellenverzeichnis und weiterführende Links

- Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe - Cloud Computing, Version 1.0, 26. September 2011
- eGovernment Schweiz, Cloud Computing Strategie der Schweizer Behörden 2012-2020, 25. Oktober 2012
- ARTIKEL-29-DATENSCHUTZGRUPPE, Stellungnahme 05/2012 zum Cloud Computing, 1. Juli 2012
- Entschliessung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 28./29. September 2011, München
- Thilo Weichert, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Cloud Computing und Datenschutz
- Philipp Mittelberger, Gabriele Binder, Datenschutzrechtliche Chancen und Risiken von Cloud Computing, in: Jus & News 2011/2, S. 163 ff.
- Datenschutzstelle Fürstentum Liechtenstein, Cloud Computing und Datenschutz, Häufig gestellte Fragen
- European Network and Information Security Agency (ENISA), Cloud Computing, Benefits, risks and recommendations for information security, November 2009
- Bundesamt für Sicherheit in der Informationstechnik (BSI), Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestsicherheitsanforderungen in der Informationssicherheit, 2011
- BSI, Spezifische Massnahmen zur Trennung der Datenbestände, ‚Gefährdungen und Gegenmaßnahmen beim Einsatz von VCE Vblock', Version 2.5, 22. Dezember 2011