dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Cloud Computing

1 Einleitung

Dieses Merkblatt richtet sich an die öffentlichen Organe im Kanton Zürich, die Cloud Services evaluieren oder 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, vom Gesetz geforderte Bestimmungen spezielles Augenmerk zu richten.

Ausgangspunkt der Nutzung solcher Cloud Services ist eine Risikoanalyse im Rahmen der Datenschutz-Folgenabschätzung gemäss § 10 Abs. 1 Gesetz über die Information und den Datenschutz (IDG, LS 170.4), 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. Siehe dazu das Merkblatt Datenschutz-Folgenabschätzung und das Formular Datenschutz-Folgenabschätzung.

2 Cloud Computing und Outsourcing

Die Inanspruchnahme von Cloud Services ist ein «Bearbeiten im Auftrag» gemäss § 6 IDG i.V.m. § 25 Verordnung über die Information und den Datenschutz (IDV, LS 170.41) und muss sich deshalb an diesen Voraussetzungen orientieren (siehe Leitfaden Bearbeiten im Auftrag). Öffentliche Organe dürfen Cloud Services nutzen, wenn sie in der Lage sind, ihre Pflichten in Bezug auf Datenschutz und Informationssicherheit wahrzunehmen. Sie sind für die Datenbearbeitung verantwortlich.

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

Die öffentlichen Organe führen für ihre Informatiksysteme und -anwendungen eine Risikoanalyse im Rahmen der Datenschutz-Folgenabschätzung durch. Je nach Gefährdungspotenzial erfolgt die Einstufung in eine der drei Sicherheitsstufen. Anschliessend werden die Schutzziele ermittelt. 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.

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

- Wahrnehmung der Verantwortung durch beide Parteien
- Anwendung schweizerischen Rechts und Vereinbarung eines schweizerischen Gerichtsstand
- Möglicher Einfluss ausländischer Rechtsordnungen
- Verlust der Kontrolle oder Verunmöglichung 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

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 gemäss§ 6 IDG auch in einer Cloud-Struktur wahrnehmen können. Es ist deshalb detailliert und schriftlich in einem Vertrag festzuhalten, wer wofür im Sinne des IDG verantwortlich zeichnet (siehe Ziff. 7 Checkliste «Vorgehen» und Ziff. 8 Anhang 1 «Überblick AGB und Vertragsbestimmungen» im Leitfaden Bearbeiten im Auftrag). Den folgenden Punkten ist besondere Beachtung zu schenken.

4.1 Kontrolle

Die Kontrollrechte des öffentlichen Organs sowie unabhängiger Aufsichtsbehörden (Datenschutzbeauftragte/Finanzkontrolle) sind zu verankern. Dies betrifft insbesondere auch die Kontrollmöglichkeit vor Ort. Die Kontrollrechte gelten von Gesetzes wegen, auch wenn sich der Auftragnehmer weigert, diese im Vertrag festzuhalten.

Weiter ist der Cloud-Anbieter zu verpflichten, regelmässig 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 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.

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 vom öffentlichen Organ bewilligt werden.

4.4 Gleichwertiges Datenschutzniveau

Datenbekanntgaben ins Ausland unterliegen den Bestimmungen von § 19 IDG. Diese gelten analog 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. Siehe Leitfaden CLOUD Act.

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. Allenfalls kann eine Informationspflicht auf der Website mit möglicher Kündigung innerhalb einer angemessenen Frist als Auffanglösung dienen. Diese Unter-Auftragnehmer müssen verpflichtet werden, Weisungen des Cloud-Anbieters zu beachten.

4.6 Anwendbares Recht und Gerichtsstand

Es ist festzuhalten, dass schweizerisches Recht, insbesondere das IDG, anwendbar ist. Weiter muss ein Gerichtsstand in der Schweiz vereinbart werden.

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 § 7 IDG geforderten, nicht abschliessend aufgezählten Schutzziele garantieren. In einem Informationssicherheitskonzept hat er die organisatorischen und technischen Sicherheitsmassnahmen wie kryptografische Verfahren, Identity- und Accessmanagement, Notfallmanagement usw. festzuhalten (siehe Übersicht Verschlüsselung der Daten im Rahmen der Auslagerung). Beim Bearbeiten von besonderen Personendaten 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 (siehe Ziff. 9 Anhang 2 «Übersicht Informationssicherheitsmassnahmen» im Leitfaden Bearbeiten im Auftrag).

5 Umsetzung der Massnahmen

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

6 Quellenverzeichnis und weiterführende Links

Datenschutzbeauftragte des Kantons Zürich
- Leitfaden Bearbeiten im Auftrag
- Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
- Leitfaden CLOUD Act

Privatim – Konferenz der schweizerischen Datenschutzbeauftragten
- Merkblatt Cloud Computing im Schulbereich
- Merkblatt «Cloud-spezifische Risiken und Massnahmen»

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Deutschland)
- Orientierungshilfe – Cloud Computing, Version 2.0

Bundesamt für Sicherheit in der Informationstechnik (BSI, Deutschland)
- Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestanforderungen in der Informationssicherheit, Eckpunktepapier, Februar 2012
- Sichere Nutzung von Cloud-Diensten, August 2016
- Baustein B 1.17 Cloud Nutzung
- Baustein B 3.303 Speicherlösungen / Cloud Storage
- Baustein B 3.304 Virtualisierung
- Baustein Cloud Management

Links zu weiterführenden Informationen
- Marit Hansen, Vertraulichkeit und Integrität der Daten und IT-Systeme im Cloud-Zeitalter
- Thilo Weichert, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Cloud Computing aus datenschutzrechtlicher Sicht
- European Union Agency for Network and Information Security (enisa), Cloud Computing Risk Assessment

V 1.5 / April 2021