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

Merkblatt

CLOUD COMPUTING IM SCHULBEREICH

1 Einleitung

Dieses Merkblatt richtet sich an Schulen, welche die Nutzung von Cloud-Services, beispielsweise Dropbox, Microsoft Office 365 oder Google Drive, evaluieren oder bereits nutzen.

Erfolgt die Datenbearbeitung in einer Cloud, ist das ein „Bearbeiten im Auftrag“, auch als „Auslagerung“ oder „Outsourcing“ bekannt. Die Risiken sind dabei wesentlich höher als bei einer konventionellen Auftragsbearbeitung, weshalb den „Cloud-inhärenten“ Faktoren wie beispielsweise dem Speichern der Daten an verschiedenen Orten und der Bearbeitung durch Unterauftragnehmer besondere Aufmerksamkeit zu schenken ist. Zudem sind vor der Nutzung solcher praktischer Dienstleistungen Rechtsfragen zu klären. So können etwa Geheimhaltungspflichten wie das Berufsgeheimnis der Datenbearbeitung in einer Cloud entgegenstehen.

Dieses Merkblatt zeigt auf, welche rechtlichen Voraussetzungen gelten, welche Fragen im Vorfeld der Nutzung solcher Cloud-Services gestellt und welche Massnahmen umgesetzt werden müssen.

2 Rechtliche Voraussetzungen

Für die Nutzung eines Cloud-Services gelten die Voraussetzungen der (Informations- und) Datenschutzgesetze betreffend das „Bearbeiten im Auftrag“. Ob der Cloud-Service zum Speichern von Daten, zum Vereinfachen der Kommunikation oder der Kooperation genutzt wird, spielt keine Rolle. Wesentlich ist, dass die einen solchen Dienst nutzende Schule in der Lage ist, ihre Pflichten in Bezug auf Datenschutz und Informationssicherheit wahrzunehmen, denn sie bleibt für die Datenbearbeitung verantwortlich.

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

Von der Auswahl bis zur Nutzung eines Cloud-Services können grundsätzlich fünf Schritte unterschieden werden:

- Prüfen, ob die Daten durch Auftragnehmer bearbeitet werden dürfen
- Prüfen, ob die Daten „Cloud-tauglich“ sind
- Auswahl des Cloud-Services und des –Anbieters
- Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB
- Umsetzung der Massnahmen

3 Vorgehen

3.1 Prüfen, ob die Daten durch Auftragnehmer bearbeitet werden dürfen

Wird die Nutzung eines Cloud-Services in Betracht gezogen, ist als Erstes zu prüfen, ob einer solchen Auftragsdatenbearbeitung rechtliche Bestimmungen oder Vereinbarungen entgegenstehen. Zu denken ist an besondere Geheimhaltungspflichten wie beispielsweise das Berufsgeheimnis im Bereich der Schulpsychologie.

Daten mit einer besonderen Geheimhaltungspflicht dürfen in eine Cloud ausgelagert werden, wenn die Vertraulichkeit so gewährleistet wird, dass durch Verschlüsselung der Cloud-Anbieter nicht auf die Daten zugreifen kann.

3.2 Prüfen, ob die Daten „Cloud-tauglich“ sind

Bei der Prüfung, ob die Daten „Cloud-tauglich“ sind, steht vor allem die Sensitivität der Daten im Vordergrund.

Die Schule muss das Gefährdungspotential sowie die Schutzziele insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität ermitteln. D.h. Daten dürfen nicht unberechtigten Dritten zugänglich sein, verloren gehen und unbefugt abgeändert werden können. Aus diesen Beurteilungen resultieren die Anforderungen an den Cloud-Service respektive den –Anbieter.

Grundsätzlich gilt für die Anforderungen die Kaskade Sachdaten, Personendaten, besonders schützenswerte Personendaten, d.h. je sensitiver die Daten, desto umfangreicher sind die organisatorischen, technischen und rechtlichen Anforderungen, die der Cloud-Service zu erfüllen hat. Gerade standardisierte Produkte können oft nicht so angepasst werden, dass sie die Rahmenbedingungen der Schulen erfüllen.

3.3 Auswahl des Cloud-Services und des –Anbieters

Stehen der Datenbearbeitung in der Cloud keine Geheimhaltungspflichten entgegen, ist der Schutzbedarf bestimmt und sind die Massnahmen definiert, kann allenfalls ein Cloud-Service ausgewählt werden.

Der Cloud-Anbieter kann aufgefordert werden, darzulegen, wie die für die Schule geltenden Rahmenbedingungen erfüllt werden können, respektive welches die rechtlichen, organisatorischen und technischen Rahmenbedingungen der angebotenen Dienstleistung sind. Bei der Auswahl können auch Zertifikate oder Auditberichte von unabhängigen Stellen behilflich sein.

Häufig ist es aber so, dass die Nutzung von Standardprodukten daran scheitert, dass keine Verträge vereinbart werden können oder auch die Nutzungsbedingungen die datenschutzrechtlichen Anforderungen nicht erfüllen und keine Abweichungen möglich sind.

3.4 Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB

Erforderlich ist grundsätzlich ein schriftlicher Vertrag zwischen der Schule und dem Cloud-Anbieter. Um der technologischen Entwicklung Rechnung zu Tragen, ist auch das Akzeptieren der Nutzungsbedingungen, respektive der AGB möglich. Diese dürfen jedoch nicht einseitig durch den Anbieter abänderbar sein.

Die Anforderungen an den Inhalt des Vertrages respektive der Nutzungsbedingungen werden in den (Informations- und) Datenschutzgesetzen konkretisiert. Geregelt sein muss insbesondere:

- der Gegenstand und Umfang der Datenbearbeitung
- die Verantwortung (wer ist wofür verantwortlich)
- die Verfügungsmacht (muss bei der Schule liegen)
- die Zweckbindung (Daten dürfen nur für die Zwecke der Schule bearbeitet werden)
- die Geheimhaltungsverpflichtungen
- die Rechte der Betroffenen (das Auskunftsrecht sowie die Durchsetzung des Rechts auf Berichtigung und Löschung müssen vertraglich garantiert werden).
- die Kontrollmöglichkeit der Schule oder externer Prüfstellen
- die Informationssicherheitsmassnahmen (für die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit).
- die Unterauftragsverhältnisse (Offenlegung und Änderung nur mit Bewilligung der Schule)
- bei einer Bearbeitung im Ausland (entweder gleichwertiges Datenschutzniveau oder es sind zusätzliche Massnahmen zu vereinbaren)
- die Orte der Datenbearbeitung (Orte müssen bekannt sein und Ortswechsel gemeldet und von der Schule bewilligt werden)
- das anwendbare Recht (es muss schweizerisches Recht vereinbart werden)
- der Gerichtsstand (es muss ein schweizerischer Gerichtsstand vereinbart werden)

3.5 Umsetzung der Massnahmen

Die Umsetzung der organisatorischen, technischen und rechtlichen Rahmenbedingungen, wie im Vertrag oder in den Nutzungsbedingungen festgehalten, muss durch die Schule laufend überprüft werden. Dabei können, wie erwähnt, auch Berichte von unabhängigen Prüfstellen oder Zertifikate in Anspruch genommen werden

4 Weitere Informationen

privatim – Merkblatt Cloud Computing (Juli 2013)

V 1.0 / Oktober 2013