dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Online Speicherdienste

1 Einleitung

Online Speicher, oft auch Online Storage, Cloud Speicher oder Cloud Storage genannt, bieten Anwendern die Möglichkeit, Daten im Internet bzw. in einer sogenannten Cloud aufzubewahren und unabhängig von ihrem Aufenthaltsort darauf zuzugreifen.

Die Nutzung von „Cloud-basierten“ Online Speicherdiensten wie z.B. Dropbox, Wuala, CloudMe, TeamDrive, Telekom Mediencenter, Microsoft Skydrive oder Google Drive ist einfach, führt aber zu erhöhten Risiken betreffend Verletzungen der datenschutzrechtlichen Rahmenbedingungen und damit zusammenhängend Verletzungen der Persönlichkeitsrechte. Diese sind bei einer Evaluation und Nutzung zu berücksichtigen.

Dieses Merkblatt enthält eine Übersicht der wichtigsten datenschutzrechtlichen Anforderungen inklusive einer diesbezüglichen Analyse einer Auswahl der bekanntesten Anbieter von solchen Online Speichern.

2 Rechtliche Voraussetzungen

Die Nutzung eines „Cloud-basierten“ Online Speichers ist eine Auslagerung der Datenbearbeitung i.S.v. § 6 IDG. Die entsprechenden Voraussetzungen des § 6 IDG sowie des konkretisierenden § 25 IDV müssen geprüft und umgesetzt werden. Vorab anzumerken ist, dass das öffentliche Organ für die Bearbeitung der Informationen bei der Nutzung solcher Online Speicher verantwortlich bleibt.

Bevor ein „Cloud-basierter“ Online Speicher genutzt werden kann, ist als erstes die Frage zu beantworten, ob die Datenbearbeitung ausgelagert werden darf, d.h. insbesondere, ob einer Auslagerung Geheimnispflichten entgegenstehen (Bsp. Berufsgeheimnisse). Weiter ist zu prüfen, ob die Daten „Cloud-tauglich“ sind. Diesbezüglich stehen vor allem die Sensitivität der Daten und die damit verbundenen Risiken

und Massnahmen im Vordergrund. Als Nächstes ist der Schutzbedarf zu definieren, d.h. die Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität sind festzulegen. Das Auslagern von Bearbeitungen besonderer Personendaten erfordert zusätzliche Massnahmen, welche dem dadurch entstehenden erhöhten Risiko Rechnung tragen (beispielsweise Verschlüsselungsmassnahmen).

Erforderlich für die Auslagerung ist grundsätzlich ein schriftlicher Vertrag zwischen dem öffentlichen Organ und dem Anbieter, in welchem insbesondere der Umgang mit Personendaten betreffend die Verantwortung, Verfügungsmacht und Zweckbindung, aber auch die Geheimhaltungsverpflichtungen, Informationssicherheitsmassnahmen und Kontrollen verankert werden. Werden Daten in einer Cloud bearbeitet, sind zusätzliche Massnahmen, beispielsweise Informationspflichten über die Bearbeitungsorte, zu vereinbaren. Werden die Daten durch den Anbieter im Ausland bearbeitet, müssen die dadurch entstehenden Risiken allenfalls durch zusätzliche Massnahmen analog derjenigen in § 19 IDG und § 22 IDV umgesetzt werden. Die Anforderungen werden in den vom Datenschutzbeauftragten zur Verfügung gestellten „AGB Auslagerung Informatikleistungen“ konkretisiert (abrufbar unter www.datenschutz.ch / Organisation und Technik).

Kann mit dem Anbieter kein schriftlicher Vertrag, wie dies bei der Nutzung von „Cloud-basierten“ Online-Speichern oft der Fall ist, abgeschlossen werden, sind die Vertrags-, respektive Nutzungsbedingungen mit Blick auf die datenschutzrechtlichen Anforderungen zu prüfen. Nur wenn diese erfüllt werden und nicht einseitig durch den Anbieter abgeändert werden können, sind sie IDG-konform.

3 Risiken

Bei der Speicherung der Daten in einer Cloud ergeben sich insbesondere folgende Risiken:

- Datenverlust
- Verlust der Verfügbarkeit
- Verlust der Vertraulichkeit
- Verlust der Integrität
- Nichtdurchsetzbarkeit des Löschens
- Unsichere Clientsoftware

4 Analyse einer Auswahl bekanntester Speicherdienste

Die Beurteilungen beziehen sich auf den Standardumfang des Dienstes. Der Funktionsumfang kann teilweise mit zusätzlicher Software (z.B. Verschlüsselungslösungen) ergänzt werden.

Massnahmen	ownCloud	Dropbox	Wuala	SecureSafe	GoogleDrive	SkyDrive	iCloud	TeamDrive
Verschlüsselte Ablage	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja
Verschlüsselter Transport	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ausschliesslicher Zugriff Datenherr / Verschlüsselung auf Client	Ja	Nein	Ja	Ja	Nein	Nein	Nein	Ja
Datenstandort	Lokal	USA	EU	CH	USA	USA	USA	EU / Lokal
Logging Zugriffe	Ja[1]	Ja	Nein	Ja	Ja	Nein	Nein	Ja
Starke Authentifizierung	Nein	Ja	Nein	(Ja)[2]	Ja	Ja	Nein[3]	Nein
SLA	-	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Schriftlicher Vertrag	-	Nein	Nein	Nein	Nein	Nein	Nein	(Ja)[4] / -

5 Weiterführende Informationen

Bundesamt für Sicherheit in der Informationstechnik – Überblickspapier Online Speicher (November 2012)

Merkblatt Cloud Computing des Datenschutzbeauftragten des Kantons Zürich (August 2012)

V 1.0 / Oktober 2013

[1] Nicht in allen Versionen
[2] Nur bei der Initialisierung
[3] In der Schweiz noch nicht verfügbar / nicht bei jedem Anmeldevorgang möglich
[4] Nach deutschem Bundesdatenschutzgesetz

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
Fax 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch