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 respektive in einer sogenannten Cloud aufzubewahren und unabhängig von ihrem Aufenthaltsort darauf zuzugreifen.

Die Nutzung von «Cloud-basierten» Online Speicherdiensten wie zum Beispiel Dropbox, CloudMe, TeamDrive, Microsoft OneDrive 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, das heisst insbesondere, ob einer Auslagerung Geheimnispflichten entgegenstehen (beispielsweise 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, das heisst 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 / Weitere Themen / Outsourcing).

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 wie beispielsweise Verschlüsselungslösungen (Boxcryptor, Truecrypt etc.) ergänzt werden.

Massnahmen	ownCloud	Dropbox	SecureSafe	Google Drive	OneDrive	iCloud	TeamDrive	Storebox	Tresorit
Verschlüsselte Ablage	Ja	Ja	Ja	Ja	Nein / Ja[1]	Ja	Ja	Ja	Ja
Verschlüsselter Transport	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Verschlüsselung auf Client	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Nein	Ja
Datenstandort	Lokal	USA	CH	USA	USA	USA	EU / Lokal	CH	EU
Logging Zugriffe	Ja[2]	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja
Starke Authentifizierung	Ja[3]	Ja	(Ja)[4]	Ja	Ja	Ja	(Ja)[5]	Ja	Ja
Schriftlicher Vertrag	-[6]	Nein	Nein	Nein	Nein	Nein	(Ja)[7] / -	(Nein)[8]	Nein

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 1.2 / Oktober 2015

1 Nur im Rahmen der Business-Lösung
2 Nicht in allen Versionen
3 Mit Zusatzsoftware (z.B. Google Authenticator App, FreeOTP, Yubikey etc.) möglich
4 Nur bei der Initialisierung per SMS
5 Mit Zusatzsoftware möglich
6 Nicht erforderlich, falls lokal installiert
7 Nach deutschem Bundesdatenschutzgesetz
8 Für Grosskunden möglich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
Fax 043 259 51 38

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