dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Online-Speicherdienste

1 Einleitung

Online-Speicherdienste, oft auch Online Storage, Cloud-Speicher oder Cloud Storage genannt, bieten Anwenderinnen und 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, TeamDrive, Microsoft OneDrive oder Google Drive ist einfach, führt aber zu erhöhten Risiken betreffend Verletzungen der datenschutzrechtlichen Rahmenbedingungen und damit zusammenhängend der Persönlichkeitsrechte. Diese sind bei einer Evaluation und Nutzung zu berücksichtigen.

Dieses Merkblatt enthält eine Übersicht der wichtigsten datenschutzrechtlichen Anforderungen inklusive einer diesbezüglichen Analyse der bekanntesten Anbieter solcher Online-Speicherdienste.

2 Rechtliche Voraussetzungen

Die Nutzung eines Cloud-basierten Online-Speicherdienstes ist eine Auslagerung der Datenbearbeitung im Sinne von § 6 IDG. Die Voraussetzungen des § 6 IDG sowie des § 25 IDV müssen geprüft und umgesetzt werden. Das öffentliche Organ bleibt für die Datenbearbeitung bei der Nutzung von Online-Speicherdienste verantwortlich.

Bevor ein Cloud-basierter Online-Speicherdienste 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 Sensitivität der Daten und die damit verbundenen Risiken und Massnahmen eine Auslagerung in die Cloud zulassen. Als Nächstes ist der

Schutzbedarf zu definieren, das heisst die Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität sind festzulegen. Die Auslagerung von Bearbeitungen besonderer Personendaten erfordert zusätzliche Massnahmen, welche dem dadurch entstehenden erhöhten Risiko Rechnung tragen, beispielsweise Verschlüsselungsmassnahmen. Siehe Übersicht Verschlüsselung der Datenablage im Rahmen der Auslagerung.

Bei der Auslagerung ist ein schriftlicher Vertrag zwischen dem öffentlichen Organ und dem Aufragnehmenden erforderlich, in dem 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 Auftragnehmenden 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 AGB Auslagerung Informatikleistungen konkretisiert.

Kann mit dem Auftragnehmenden kein schriftlicher Vertrag 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 Auftragnehmenden geändert werden können, sind sie IDG-konform.

3 Risiken

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

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

4 Analyse bekannter Online-Speicherdienste

Die Beurteilungen beziehen sich auf den Standardumfang des Dienstes. Der Funktionsumfang kann teilweise mit zusätzlicher Software wie beispielsweise Verschlüsselungslösungen (Boxcryptor, Cryptomator, Veracrypt etc.) ergänzt werden.

Speicherdienst / Anforderung	Dropbox	Google Drive	iCloud	own-Cloud	One-Drive	Secure-Safe	Storebox	Team-Drive	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[2]	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja
Datenstandort	USA	USA	USA	Lokal	USA	CH	CH	EU / Lokal	EU
Logging Zugriffe	Ja	Ja	Nein	Ja[3]	Nein	Ja	Ja	Ja	Ja
Starke Authentifizierung	Ja	Ja	Ja	Ja[4]	Ja	(Ja)[5]	Ja	(Ja)[6]	Ja
Schriftlicher Vertrag[7]	Nein	Nein	Nein	-[8]	Nein	Ja[9]	(Nein)[10]	(Ja)[11] / -	Nein

1 Nur im Rahmen der Business-Lösung
2 Der Schlüssel wird durch die Software des Auftragnehmenden (AN) verarbeitet und kann durch ihn kompromittiert werden.
3 Nicht in allen Versionen
4 Mit Zusatzsoftware (z.B. FreeOTP, Yubikey etc.) möglich
5 Nur bei der Initialisierung per SMS
6 Mit Zusatzsoftware möglich
7 Alternativ können datenschutzkonforme AGB akzeptiert werden. Diese dürfen nicht einseitig abänderbar sein.
8 Nicht erforderlich, falls lokal installiert
9 Es existiert eine Rahmenvereinbarung zwischen DSwiss AG und dem Verein Schweizerische Städte- und Gemeindeinformatik (SSGI) vom 13. Dezember 2015. Basierend darauf können öffentliche Organe, die Mitglieder des SSGI sind, individuelle Nutzungsverträge abschliessen.
10 Für Grosskunden möglich
11 Nach deutschem Bundesdatenschutzgesetz

5 Weiterführende Informationen

Datenschutzbeauftragter des Kantons Zürich

- Leitfaden Bearbeiten im Auftrag
- Merkblatt Cloud Computing
- Übersicht Verschlüsselung der Datenablage im Rahmen der Auslagerung

Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland

- Überblickspapier Online-Speicher

V 1.6 / Juli 2018

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh