dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Online-Speicherdienste

1 Einleitung

Die Online-Speicherdienste werden auch als Online Storage, Cloud-Speicher oder Cloud Storage bezeichnet. Die bekanntesten Beispiele sind Dropbox, Microsoft Onedrive oder Google Drive. Dabei werden die Daten auf den Servern des Diensteanbieters gespeichert. Die Anwenderinnen und Anwender können weltweit übers Internet darauf zugreifen.

Die Cloud-basierten Online-Speicherdienste sind sehr einfach zu nutzen. Die datenschutzrechtlichen Rahmenbedingungen sind problematisch. Die Persönlichkeitsrechte sind erhöhten Risiken ausgesetzt.

Dieses Merkblatt enthält eine Übersicht der wichtigsten datenschutzrechtlichen Anforderungen sowie eine Analyse der bekanntesten Online-Speicherdienste.

2 Rechtliche Voraussetzungen

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

Zuerst muss abgeklärt werden, ob die Datenbearbeitung ausgelagert werden darf. Sonst kann kein Online-Speicherdienst genutzt werden. Dabei ist insbesondere zu prüfen, ob einer Auslagerung Geheimnispflichten entgegenstehen, beispielsweise das Berufsgeheimnis oder ein besonderes Amtsgeheimnis.
Danach ist zu prüfen, ob die Sensitivität der Daten angesichts der Risiken eine Auslagerung in die Cloud zulassen.
Als Nächstes ist der Schutzbedarf zu definieren. Die Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität sind festzulegen. Besondere Personendaten bergen ein erhöhtes Risiko für die Persönlichkeitsrechte der betroffenen Personen. Ihre Auslagerung erfordert zusätzliche Massnahmen, beispielsweise Verschlüsselungsmassnahmen. Siehe Übersicht Verschlüsselung der Datenablage im Rahmen der Auslagerung.

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch

Bei der Auslagerung ist ein schriftlicher Vertrag zwischen dem öffentlichen Organ und dem Auftragnehmenden erforderlich. Darin muss der Umgang mit Personendaten betreffend die Verantwortung, die Verfügungsmacht und die Zweckbindung verankert werden. Zudem sind darin die Geheimhaltungsverpflichtungen, die Informationssicherheitsmassnahmen und die Kontrollen zu regeln.

- Werden die Daten in einer Cloud bearbeitet, sind zusätzliche Massnahmen zu vereinbaren, beispielsweise die Informationspflichten über die Bearbeitungsorte,.
- Werden die Daten durch den Auftragnehmenden im Ausland bearbeitet, müssen allenfalls zusätzliche Massnahmen umgesetzt werden (§ 19 IDG und § 22 IDV). 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 die Anforderungen erfüllt werden und die Nutzungsbedingungen 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	Next-cloud	Onedrive	Secure-Safe	Team-drive	Tresorit
Verschlüsselte Speicherung[1]	Ja	Ja	Ja	Ja	Nein / Ja[2]	Ja	Ja	Ja
Verschlüsselter Transport	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Verschlüsselung auf Client	Nein[3]	Nein[3/4]	Ja[5/5]	Ja	Nein	Ja[5]	Ja[5]	Ja[5]
Datenstandort	USA	USA	USA	Lokal	USA	CH	EU / Lokal	EU
Aufzeichnung der Zugriffe von Mitarbeitenden (Logging)	Ja	Ja	Ja[6]	Ja	Ja[7]	Ja	Ja	Ja
Starke Authentifizierung	Ja	Ja	Ja	Ja[8]	Ja	(Ja)[9]	(Ja)[10]	Ja
Quellcode einsehbar (OpenSource)	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein

5 Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich

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

V 1.9 / Oktober 2024

[1] Serverseitig

[2] Nur im Rahmen der Business-Lösung

[3] Nur für Firmenkunden

[4] Ende-zu-Ende-Verschlüsselung. Der Schlüssel verbleibt bei den Kunden. Die Auftragnehmenden haben grundsätzlich keinen Zugriff auf die Daten. Sie könnten über den verwendeten Client jedoch theoretisch darauf zugreifen.

[5] Kunden müssen die Ende-zu-Ende-Verschlüsselung (E2EE) selbst aktivieren.

[6] Nur für Firmenkunden

[7] Nur für Firmenkunden

[8] Mit zusätzlicher App möglich

[9] Nur bei der Initialisierung per SMS

[10] Mit Zusatzsoftware möglich