



**dsb**

datenschutzbeauftragte  
des kantons zürich

## Merkblatt

---

# Nutzung der Cloud-Produkte von US-Unternehmen

## 1 Ausgangslage

Dieses Merkblatt richtet sich an öffentliche Organe im Kanton Zürich, die beabsichtigen, Cloud-Produkte von Unternehmen mit Bezug zu den USA wie Microsoft, Google oder Amazon Web Services (AWS) einzusetzen. Die Nutzung solcher Dienste stellt rechtlich eine Auslagerung der Datenbearbeitung gemäss § 6 Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](#)) dar. Unternehmen mit US-Bezug unterstehen dem CLOUD Act (Clarifying Lawful Overseas Use of Data Act). Die Anwendbarkeit des CLOUD Acts hat folgende Auswirkungen:

- **Zugriff durch US-Behörden:** Der CLOUD Act kann Anbieter von Cloud-Produkten mit Bezug zu den USA verpflichten, amerikanischen Behörden Zugriff auf Personendaten zu gewähren, selbst wenn die Personendaten ausserhalb der USA (zum Beispiel in Rechenzentren in der Schweiz oder im EU/EFTA-Raum) gespeichert sind.
- **Umgehung der Rechtshilfe:** Die internationale Rechtshilfe regelt die Zusammenarbeit zwischen Staaten in Rechtsangelegenheiten. Sie basiert auf dem Grundsatz, dass kein Staat auf dem Territorium eines anderen Staates ohne dessen Zustimmung und Einhaltung von Rechtsschutzverfahren hoheitliche Handlungen (wie die Beschaffung von Personendaten beispielsweise im Rahmen von Beweiserhebungen) vornehmen darf. Dieser völkerrechtliche Grundsatz wird durch die Zugriffsmöglichkeit von US-Behörden auf Personendaten im Rahmen des CLOUD Acts umgangen. Da der Zugriff ohne Zustimmung und Prüfung durch den Staat erfolgt, in dem die Daten liegen, wird dessen Souveränität missachtet.
- **Erhöhtes Risiko für Grundrechte bei besonderen Personendaten:** Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, zählen zu den besonderen Personendaten (§ 3 Abs. 4 lit. a IDG). Dazu gehören Informationen über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Informationen über die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten oder Informationen über Massnahmen der sozialen Hilfe oder über strafrechtliche Verfolgungen (siehe § 3 Abs. 4 IDG). Ein faktischer Zugriff durch US-Behörden auf besondere Personendaten stellt ein erhöhtes Risiko für die Grundrechte der betroffenen Personen dar.
- **Gefährdung von Geheimnispflichten:** Bei Informationen und Personendaten, die einer besonderen Geheimnispflicht unterstehen, führt die faktische Möglichkeit eines Zugriffs von US-Behörden zu einer

Verletzung der entsprechenden Geheimnispflicht. Dazu gehören insbesondere folgende Geheimnispflichten:

- Berufsgeheimnis (Art. 321 Schweizerisches Strafgesetzbuch, [SR 312](#); § 15 Gesundheitsgesetz, [LS 810.1](#)),
- Steuergeheimnis (§ 120 Steuergesetz, [LS 631.1](#)),
- Sozialhilfegeheimnis (§ 47 Sozialhilfegesetz, [LS 851.1](#)),
- Geheimnis der Opferhilfeberatungsstellen (Art. 11 Opferhilfegesetz, [SR 312.5](#)).

Dabei gilt es zu beachten, dass Mitarbeitende von US-Unternehmen aufgrund der Konzernstruktur und der internationalen Vernetzung ihrer Arbeitgeber nicht als Hilfspersonen gelten.

## 2 Erforderliche Massnahmen

Eine Auslagerung an ein US-Unternehmen ist für besondere Personendaten nur dann datenschutzkonform, wenn das öffentliche Organ durch technische Massnahmen verhindert, dass das US-Unternehmen oder seine Tochtergesellschaften ohne Zutun des öffentlichen Organs Zugriff auf den Klartext der Personendaten erhält. Bei Informationen und Personendaten, die durch eine besondere Geheimnispflicht geschützt werden, müssen zudem auch die Randdaten vor dem Zugriff des US-Unternehmens geschützt werden.

Für einen genügenden Schutz kommen folgende Lösungen in Frage:

- **Cloud Access Security Broker (CASB)**: Ein Drittanbieter, der nicht dem CLOUD Act untersteht, wird zwischengeschaltet. Die Verschlüsselung erfolgt so, dass der Schlüssel ausschliesslich beim öffentlichen Organ und dem CASB liegt.
- **Double Key Encryption (DKE)/Hold your own Key (HYOK)**: Hierbei werden Daten so verschlüsselt, dass das US-Unternehmen weder auf die Inhalte noch auf die Schlüssel zugreifen kann.
- **Confidential Computing**: Die Personendaten werden in einem abgeschotteten Bereich des Prozessors (Enklave) bearbeitet. Dies ermöglicht eine Verschlüsselung von Personendaten in der Cloud auch während der Bearbeitung (data in use). Selbst Administratoren des US-Unternehmens oder US-Behörden mit Systemzugriff können den Speicherinhalt während der Bearbeitung nicht auslesen.
- **Hybrides Modell/Datentrennung**: Besondere Personendaten werden ausschliesslich auf eigenen Servern des öffentlichen Organs oder bei einem Unternehmen aus der Schweiz oder dem EU/EFTA-Raum bearbeitet. Nur Personendaten und Informationen werden in der Cloud eines US-Unternehmens bearbeitet.

## 3 Vertragliche Anforderungen

Gemäss § 25 Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](#)) ist bei jeder Auslagerung ein schriftlicher Vertrag abzuschliessen. Die vorgesetzte Stelle genehmigt Aufträge für das Bearbeiten von besonderen Personendaten. Der Vertrag muss mindestens folgende Aspekte regeln:

- den Gegenstand und den Umfang der übertragenen Aufgaben,
- den Umgang mit Personendaten,
- die Geheimhaltungsverpflichtungen,
- die Behandlung von Informationszugangsgesuchen,
- die zum Schutz der Informationen vorzukehrenden Massnahmen,
- die Kontrolle der Auftrags Erfüllung,
- die bei Pflichtverletzung vorgesehenen Sanktionen,

- die Vertragsdauer und die Voraussetzungen der Vertragsauflösung.

Der Regierungsrat hat mit Beschluss vom 24. Juni 2015 (RRB 2015/0670) die Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen) für die ihm unterstellten Verwaltungseinheiten und für die Staatskanzlei für verbindlich erklärt. Sie sind zwingend als erstrangiger Bestandteil in das Vertragsverhältnis mit US-Unternehmen aufzunehmen. Allen übrigen öffentlichen Organen wird geraten, diese AGB in ihre Verträge einzubeziehen, da sie die Vorgaben des IDG direkt umsetzen.

#### **4 Verhältnis zum Swiss-US Data Privacy Framework**

Der Angemessenheitsbeschluss des Bundesrates attestiert zertifizierten US-Organisationen zwar ein angemessenes Datenschutzniveau. Dennoch bleibt der CLOUD Act bei der Auslagerung der Datenbearbeitung an Unternehmen mit Bezug zu den USA anwendbar. Der Angemessenheitsbeschluss ändert auch nichts daran, dass das öffentliche Organ für die Auslagerung der Datenbearbeitung im konkreten Einzelfall verantwortlich bleibt. Die Zugriffsmöglichkeiten im Rahmen des CLOUD Acts müssen weiterhin in die rechtliche Beurteilung miteinbezogen werden. Bei besonderen Personendaten oder Informationen unter einer besonderen Geheimnispflicht genügen die Standardgarantien des Frameworks ohne die oben genannten technischen Massnahmen (Verschlüsselung) nicht, um datenschutzkonform auszulagern.

#### **5 Weitere Informationen**

Weiterführende Leitfäden und Publikationen sind auf unserer Website unter der Rubrik «Auslagerung» abrufbar:

- [Leitfaden Bearbeiten im Auftrag](#)
- [Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung](#)
- [Leitfaden Auslagerung: CLOUD Act](#)
- [Leitfaden Nutzung externer Cloud-Dienste](#)
- [Merkblatt Cloud-Computing](#)

V 1.0 / Februar 2026