dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Nutzung externer Cloud-Dienste

Dieser Leitfaden richtet sich an Mitarbeitende öffentlicher Organe, die Cloud-Dienste evaluieren. Er zeigt auf, welche Punkte bei der Nutzung externer Cloud-Dienste zu berücksichtigen sind und wie bei der Auswahl von Cloud-Diensten vorzugehen ist.

Der Regierungsrat hat einen Beschluss zur Nutzung von Microsoft 365 (MS 365) erlassen (RRB 542/2022 vom 30. März 2022). Darin wird festgehalten, dass für die Einführung von Cloud-Lösungen keine Rechtsgrundlagen geändert oder geschaffen werden müssen, sondern die geltenden Bestimmungen einzuhalten sind.

Die Informationen zu den geltenden Bestimmungen sind in den folgenden Publikationen beschrieben:
- Merkblatt Cloud Computing
- Leitfaden Bearbeiten im Auftrag, insbesondere Checklisten Seiten 10, 11 und 12
- Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
- Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud-Nutzung unter Berücksichtigung des CLOUD Act
- AGB Auslagerung Informatikleistungen

Die Nutzung von externen Cloud-Diensten ist aus datenschutzrechtlicher Sicht ein Bearbeiten im Auftrag (§ 6 IDG i.V.m. § 25 IDV). Dies bedeutet für das öffentliche Organ, dass es dieselbe Verantwortung trägt, wie wenn es die Informationen selbst bearbeiten würde (§ 6 Abs. 2 IDG). Das heisst, dass es auch für die Auswahl, Instruktion und Überwachung des Cloud-Anbieters verantwortlich bleibt. Cloud-Dienste können nur genutzt werden, wenn die Grundrechte der betroffenen Personen gleichwertig geschützt sind wie bei einer Datenbearbeitung durch das öffentliche Organ selbst.
Das öffentliche Organ muss einerseits evaluieren, ob gesetzliche Bestimmungen wie Geheimhaltungsvorschriften und/oder vertragliche Vereinbarungen einer Auslagerung entgegenstehen. Andererseits muss mit einer Datenschutz-Folgenabschätzung (DSFA) abgeklärt werden, welche Risiken die beabsichtigte Datenbearbeitung in der Cloud für die Grundrechte der betroffenen Personen hat und mit welchen technischen und organisatorischen Massnahmen diesen begegnet werden kann.

Vorgehensweise

1. Bestimmen der zu bearbeitenden Daten und der Art der Datenbearbeitung (Sachdaten, Personendaten oder besondere Personendaten, Bearbeitungsvorgang, Zweck und Umfang der Datenbearbeitung). Je sensitiver die Informationen, desto umfangreicher sind die rechtlichen, organisatorischen und technischen Anforderungen, die das öffentliche Organ und somit auch der Auftragnehmer zu erfüllen haben. Zudem sind andere Klassifizierungen durch das öffentliche Organ (intern, vertraulich, geheim) einzubeziehen und bei den Massnahmen entsprechend zu berücksichtigen.
   Siehe auch Leitfaden Bearbeiten im Auftrag, Checkliste Seite 10.

2. Prüfen, ob gesetzliche Bestimmungen oder vertragliche Vereinbarungen eine Auftragsdatenbearbeitung einschränken. Beispiel: Art. 12 Abs. 5 Verordnung über das elektronische Patientendossier schreibt vor, dass die Datenspeicher sich in der Schweiz befinden und dem schweizerischen Recht unterstehen müssen.
3. Prüfen, ob besondere Geheimnispflichten die Auslagerung verhindern oder besondere Massnahmen erfordern (Berufsgeheimnis, Steuergeheimnis, Sozialhilfegeheimnis, Opferhilfegeheimnis).
   Dabei ist das Rechtsumfeld des Cloud-Anbieters zu berücksichtigen, beispielsweise der CLOUD Act oder die DSGVO. Personendaten unter besonderen Geheimnispflichten können nur dann in die Cloud von Anbietern ausgelagert werden, die dem CLOUD Act unterstehen, wenn durch eine technische Lösung das Offenbaren dieser Daten ausgeschlossen werden kann. Eine Verschlüsselung der Daten, bei der das Schlüsselmanagement beim öffentlichen Organ liegt, schliesst das Offenbaren aus.
   Siehe Leitfaden CLOUD Act.
4. Mit einer DSFA prüfen, welche Risiken für die Grundrechte der betroffenen Personen durch die Datenbearbeitung in der Cloud bestehen, und definieren, mit welchen organisatorischen und technischen Massnahmen diesen begegnet respektive die Informationssicherheit gewährleistet werden kann.
   Siehe Merkblatt DSFA und Formular DSFA.
   Siehe auch Leitfaden Bearbeiten im Auftrag, Checkliste Seite 12 und Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung.
5. Erstellen eines ISDS-Konzepts nach der Hermes-Methode
   Mitarbeitende der kantonalen Verwaltung finden Ausführungen zum ISDS im Intranet.
6. Bei besonderen Risiken für die Grundrechte der betroffenen Personen die beabsichtigte Datenbearbeitung der Datenschutzbeauftragten zur Vorabkontrolle einreichen. Dies trifft beispielsweise zu, wenn viele besondere Personendaten bearbeitet, neue Technologien eingesetzt werden oder eine grosse Anzahl Personen betroffen ist.
7. Analyse der vertraglichen Vorgaben oder der AGB des Anbieters. Zu berücksichtigen sind die datenschutzrechtlichen Anforderungen, die dem Cloud-Anbieter inhaltlich zu überbinden sind. Diese sind in den AGB Auslagerung Informatikleistungen enthalten. Anforderungen bestehen beispielsweise an die Zweckbindung, die Bekanntgabe der Daten an Dritte, den Ort der Datenbearbeitung, die Unterauftragsverhältnisse, das Kontrollrecht, das anwendbare Recht, den Gerichtsstand sowie die Informationssicherheitsmassnahmen wie Transport- und Speicherverschlüsselung, Zwei-Faktor-Authentifizierung usw.
   Für die Übersicht siehe Leitfaden Bearbeiten im Auftrag, Seite 11.
8. Bei besonderen Personendaten prüfen, ob eine vertragliche Lösung betreffend Verschlüsselung umgesetzt werden muss.
   In einer vertraglichen Lösung verpflichtet sich der Auftragnehmer, den Schlüssel nur auf ausdrückliche Anfrage und nach ausdrücklicher Einwilligung des Auftraggebers einzusetzen, um auf die Daten zuzugreifen.
   Siehe Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung.
9. Einbeziehen von Rahmenverträgen, beispielsweise
   - Rahmenvertrag SIK/Digitale Verwaltung Schweiz mit Microsoft betreffend schweizerischen Gerichtsstand und schweizerisches Recht für Datenschutzbelange
   - Educa- oder Switch-Rahmenvertrag für die Nutzung von MS 365 im Bildungsbereich
   - Educa- oder Switch-Rahmenvertrag für Google Workspace im Bildungsbereich
   - Apple Side Letter für die Nutzung von Apple School Manager.
10. Einschliessen der EU-Standardvertragsklauseln mit Anpassungen an das schweizerische Recht bei Anbietern aus Ländern mit nicht angemessenem Datenschutzniveau, beispielsweise USA
11. Schweizerische oder europäische Clouds oder solche in Ländern, die über einen gleichwertigen gesetzlichen Datenschutz verfügen, sind zu bevorzugen. Ansonsten sind angemessene zusätzliche Informationssicherheitsmassnahmen umzusetzen.
12. Bei besonderen Personendaten Entscheid durch vorgesetzte Behörde einholen.

13. Produkte mit strategischer Bedeutung in der kantonalen Verwaltung dem Regierungsrat zur Zustimmung vorlegen.
14. Umsetzen der organisatorischen und technischen Massnahmen durch das öffentliche Organ, die sich aufgrund der Sensitivität der Daten, der Geheimnispflichten sowie des Rechtsumfeldes des Anbieters ergeben. Die Massnahmen müssen angemessen sein. Eine Cloud-Lösung darf nicht zu einem höheren Risiko für die betroffenen Personen führen als eine bisherige lokale Lösung.
    Dafür ist ein Nutzungskonzept zu erstellen, sind Massnahmen durch Nutzer zu definieren, datenschutzfreundliche Einstellungen umzusetzen sowie Verschlüsselung oder andere technische Massnahmen vorzunehmen, um die Kenntnisnahme von Daten auszuschliessen, die aufgrund von Geheimnispflichten dem Anbieter nicht offengelegt werden dürfen usw.
    Eine Anleitung zur Erstellung eines Nutzungskonzepts findet sich im Leitfaden MS 365 im Bildungsbereich Ziff. 3.

Weitere Möglichkeiten

Überlegungen zu den folgenden Möglichkeiten sind in den Evaluationsprozess einzubeziehen, um den erforderlichen Schutz für die Daten zu erreichen:

- On-premise-Lösungen
- Hybride Cloud
- Treuhänderische Cloud
- Pseudonymisieren von Personendaten
- Office 2019
- Nutzung von Produkten wie Dataport, Next Cloud prüfen
- Eingeschränkte Nutzung eines Produkts, beispielsweise nur Nutzung einzelner Dienste oder für einzelne Datenkategorien

Gesetzliche Grundlagen

§ 6 IDG i.V.m. § 25 IDV
§ 7 IDG
§ 10 IDG i.V.m. § 24 IDV
Gesetz über die Auslagerung von Informatikdienstleistungen

V 1.1 / Juni 2022