Checkliste Microsoft 365 in der Verwaltung

Bei vielen öffentlichen Organen stellt sich die Frage der Verwendung von Microsoft 365 (vormals Office 365) in der *Verwaltung*. Microsoft 365 ist eine (US)-Cloud. Damit diese Datenbearbeitung zulässig ist, müssen einige Punkte berücksichtigt werden, die nachfolgend dargelegt werden sollen. Die Zulässigkeit der Nutzung von Microsoft 365 hängt von der Art der beanspruchten Dienste, der Art und dem Umfang der bearbeiteten Personendaten und weiterer Rahmenbedingungen ab. Wichtige Voraussetzung ist eine sorgfältige Klassifizierung der Daten. Das öffentliche Organ muss zudem sorgfältig prüfen, wofür es die Verantwortung tragen kann und wofür nicht. Letztendlich geht es um das Vertrauen der Bürgerinnen und Bürger in die Datenbearbeitung der öffentlichen Organe.

Bisher stellte sich die Frage des Einsatzes von Microsoft 365 vor allem im *Schulbereich*: Hier gibt es eine Zusatzvereinbarung, die Gerichtsstand in der Schweiz und die Anwendung von Schweizer Recht vorsieht. Es dürfen keine sensiblen Personendaten bearbeitet werden und die Bearbeitung «gewöhnlicher» Personendaten ist im Umfang zu beschränken. Die Verwendung ist denn auch nur für den *schulischen* Bereich (Aufgabenblätter etc.) vorgesehen, nicht aber für den Bereich der *Schulverwaltung*. Zur Verwendung von Microsoft 365 im Schulbereich gibt es ein Merkblatt.

Wie muss das öffentliche Organ vorgehen, wenn es beabsichtigt, Microsoft 365 in der *Verwaltung* (auch *Schulverwaltung*) einzusetzen? Dazu nachfolgend eine Schritt-um-Schritt-Anleitung:

1 Sind die Voraussetzungen für eine Bearbeitung durch Dritte erfüllt?[1]

- Die Datenbearbeitung durch Dritte darf nicht durch Gesetz oder Verordnung ausgeschlossen sein;
- Der Dritte bietet Gewähr für die datenschutzrechtlich einwandfreie Bearbeitung.
- Der Dritte darf die Daten nur so bearbeiten, wie es das öffentliche Organ selbst darf nach den geltenden gesetzlichen Bestimmungen
- Die Daten müssen vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden.
- Das öffentliche Organ muss mit regelmässigen Kontrollen prüfen, ob der Datenschutz eingehalten wird.
- Die Weiterübertragung der Datenbearbeitung bedarf der vorgängigen schriftlichen Zustimmung des öffentlichen Organs.

Die Fachstelle für Datenschutz hat zur Bearbeitung durch Dritte (Outsourcing) ein Merkblatt verfasst.

1 Art. 9 Datenschutzgesetz (sGS 142.1; abgekürzt DSG).

2 Sind die Voraussetzungen für eine Datenbearbeitung in einer (US)-Cloud erfüllt?

– Anwendbares Recht / Gerichtsstand: Es muss Schweizer Recht anwendbar und der Gerichtsstand in der Schweiz sein. Dazu gibt es eine Zusatzvereinbarung, die zwischen SIK[2] und Microsoft geschlossen wurde; Diese muss unterzeichnet werden.
– Ort der Datenbearbeitung (Serverstandorte): Da Microsoft ein US-Unternehmen ist, gilt der Cloud Act; d.h., US-Behörden können auf Server ausserhalb der USA zugreifen ohne Weg über die internationale Rechtshilfe. Die Fachstelle für Datenschutz hat in ihrem Tätigkeitsbericht 2019 ausgeführt, dass sie dies für die Bearbeitung von besonders schützenswerten Personendaten und solchen die einem Berufs- oder besonderen Amtsgeheimnis unterstehen als nicht zulässig erachtet: Tätigkeitsbericht 2019. Ausnahme: Das Schlüsselmanagement liegt ausschliesslich beim öffentlichen Organ.
– Geheimnisschutz / Schlüsselmanagement: Bei besonders schützenswerten Personendaten und solchen die dem Berufs- oder einem besonderen Amtsgeheimnis unterstehen, muss das Schlüsselmanagement beim öffentlichen Organ liegen (siehe oben).
– Bearbeitung weiterer Daten (Randdaten): Für Personendaten, die beim Bearbeiten durch den Dritten anfallen, müssen dieselben Bedingungen gelten, wie für jene, welche das öffentliche Organ dem Dritten zur Verfügung stellt.

3 Gibt es weitere Risiken gemäss Merkblatt «Cloud-spezifische Risiken und Massnahmen» von privatim?

4 Ist eine Datenschutz-Folgenabschätzung erforderlich?[3]

Kann die Datenbearbeitung in Microsoft 365 zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, muss das öffentliche Organ eine Datenschutz-Folgenabschätzung machen. Diese Voraussetzung ist bei einer Bearbeitung von Personendaten in Microsoft 365 gegeben, weshalb das öffentliche Organ in jedem Fall eine solche durchführen muss. Ergibt die Datenschutz-Folgenabschätzung, dass kein hohes Risiko für die betroffenen Personen besteht, muss das öffentliche Organ das Vorhaben nicht der Datenschutzfachstelle zur Vorabkonsultation unterbreiten. Die Unterlagen müssen aber für die Beweispflicht gemäss Datenschutzgesetz (Art. 3 Abs. 3 DSG) aufbewahrt werden. Eine Datenschutz-Folgenabschätzung ist – allgemein gesagt – eine Risikoanalyse der Auswirkungen einer Datenbearbeitung auf die Grundrechte.

5 Ist eine Vorabkonsultation erforderlich?[4]

Ergibt die Datenschutz-Folgenabschätzung, dass trotz ergriffener Massnahmen ein hohes Risiko für die Grundrechte verbleibt, muss das Vorhaben der kantonalen Fachstelle oder der zuständigen Gemeindefachstelle zur Vorabkonsultation unterbreitet werden. Diese gibt eine Stellungnahme mit Empfehlungen ab. Das öffentliche Organ muss schriftlich zu Handen der Datenschutzfachstelle bestätigen, dass es die Risiken verstanden und die Verantwortung für das Restrisiko übernimmt.

---

2 Schweizerische Informatikkonferenz.
3 Art. 8a DSG.
4 Art. 8b DSG.

Kritische Punkte

Derzeit kritische Punkte bei einer allfälligen Verwendung von Microsoft 365 sind vor allem die Folgenden:

- Es ist unklar, wer der verantwortliche Vertragspartner ist: Microsoft Schweiz GmbH oder Microsoft Ireland Operations Ltd.
- Es müssen Dienste ausgewählt werden, an denen ausschliesslich zulässige Unterauftragnehmer beteiligt sind.
- Es muss darauf geachtet werden, dass die gewählten Onlineservices in der Schweiz oder in der EU geolokalisert sind. Länder ohne gleichwertiges Datenschutzniveau müssen ausgeschlossen werden. Siehe dazu Staatenliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten.
- Das Auditrecht muss eingeräumt und vom öffentlichen Organ praktikabel durchgesetzt werden können.
- Microsoft muss über sämtliche Zugriffsbegehren von (ausländischen) Behörden informieren und von sich aus alle Rechtsmittel ergreifen, um solche Begehren abzuwehren. Der zweite Punkt ist bisher nicht erfüllt.
- Microsoft schliesst ein Zugriff auf Personendaten für «legitime Geschäftstätigkeiten» nicht aus. Für solche Zugriffe fehlt es an einer Grundlage im kantonalen Gesetz, weshalb sie nicht zulässig sind.

Kontakt

- *Kanton*: Kantonale Fachstelle für Datenschutz, Tel 058 229 14 14, E-Mail: datenschutz@sg.ch
- *Gemeinden*: www.sg.ch/sicherheit/datenschutz/kontakt-weitere-datenschutzbehoerden/adressen-gemeindefachstellen.html

März 2021