Interpellation Nr. 147 (Januar 2026)
betreffend Verwendung von Copilot Chat in der Basler Verwaltung?

25.5600.01

Gemäss einem Artikel der NZZ vom 4. Januar 2026 ist seit Mai 2025 bei Computern von Angestellten der Bundesverwaltung Copilot Chat installiert. Bei diesem handelt es sich um ein Angebot von Microsoft, welches in der Regel Teil der Lizenzen ist und vom Unternehmen standardmässig eingeschaltet wird. Microsoft Copilot basiert technisch auf grossen Sprachmodellen. Im Unterschied zum klassischen LLM ist Copilot jedoch tief in die Infrastruktur von Microsoft 365 eingebunden. Eine zentrale Rolle spielt dabei das sogenannte Grounding. Beim Grounding bezieht die KI ihre Informationen und Antworten auf Basis von Unternehmensdaten aus dem Microsoft Graph. Also Informationen aus z.B. E-Mails, OneDrive-Dateien, SharePoint, Kalendern oder Teams-Chats. Copilot generiert Antworten also nicht aus einem allgemeinen Modellwissen heraus, sondern auf Basis von konkreten Informationen aus dem Unternehmenskontext. Dabei greift das Programm auf sämtliche Inhalte zu, auf die auch der jeweilige Nutzer im Microsoft-365 berechtigt ist. Dazu können sensible und vertrauliche Daten gehören. Technisch gibt es für Copilot kaum Einschränkungen, solange Nutzende selbst Zugriff auf die Inhalte haben. Fehlt ein klar strukturiertes Berechtigungs- und Lablekonzept, entsteht daraus ein erhebliches Risiko: Vertrauliche Informationen können in andere Kontexte einfliessen, etwa wenn Copilot automatisch neue Inhalte erstellt, Besprechungen zusammenfasst oder Entwürfe vorschlägt. Solche Datenübertragungen erfolgen ohne Kontextkontrolle und meist unbemerkt auch Inhalte, die ursprünglich nur für bestimmte Rollen gedacht waren, können versehentlich offengelegt werden.

Die Interpellantin bittet den Regierungsrat um die Beantwortung folgender Fragen:

1. Wo in der kantonalen Verwaltung (auch erweiterte Verwaltung wie zum Beispiel Gerichte, Parlamentsdienst und Schulen) wird Copilot verwendet? Ist geplant Copilot in der kantonalen Verwaltung zu verwenden?
2. Falls ja:
   a. Wie wird sichergestellt, dass Daten nicht an unberechtigte Dritte weitergegeben werden?
   b. Wird sichergestellt, dass Microsoft die Daten nicht für das Trainieren der KI-Lösung verwendet werden?
   c. Ist es technisch möglich Microsoft den Zugriff auf Daten für das Training von KI oder auf andere Weise zu verwehren? Ist es möglich, Copilot zu sperren oder zu deaktivieren, falls eine datenschutzkonforme Einführung nicht realisierbar ist?
   d. Wurden die Mitarbeitenden im Umgang mit Copilot geschult?
   e. Welche Weisungen für die Mitarbeitenden gibt es?
3. Da der Grosse Rat bzw. der Parlamentsdienst an IT BS angeschlossen sind:
   a. Wie wird sichergestellt, dass keine geheimen Daten aus den grossrätlichen Kommissionen in KI-Anwendungen von Microsoft gelangen?
   b. Wie wurde das Ratsbüro in den Prozess einbezogen und wie wurde der Parlamentsdienst dahingehend geschult?

Anina Ineichen