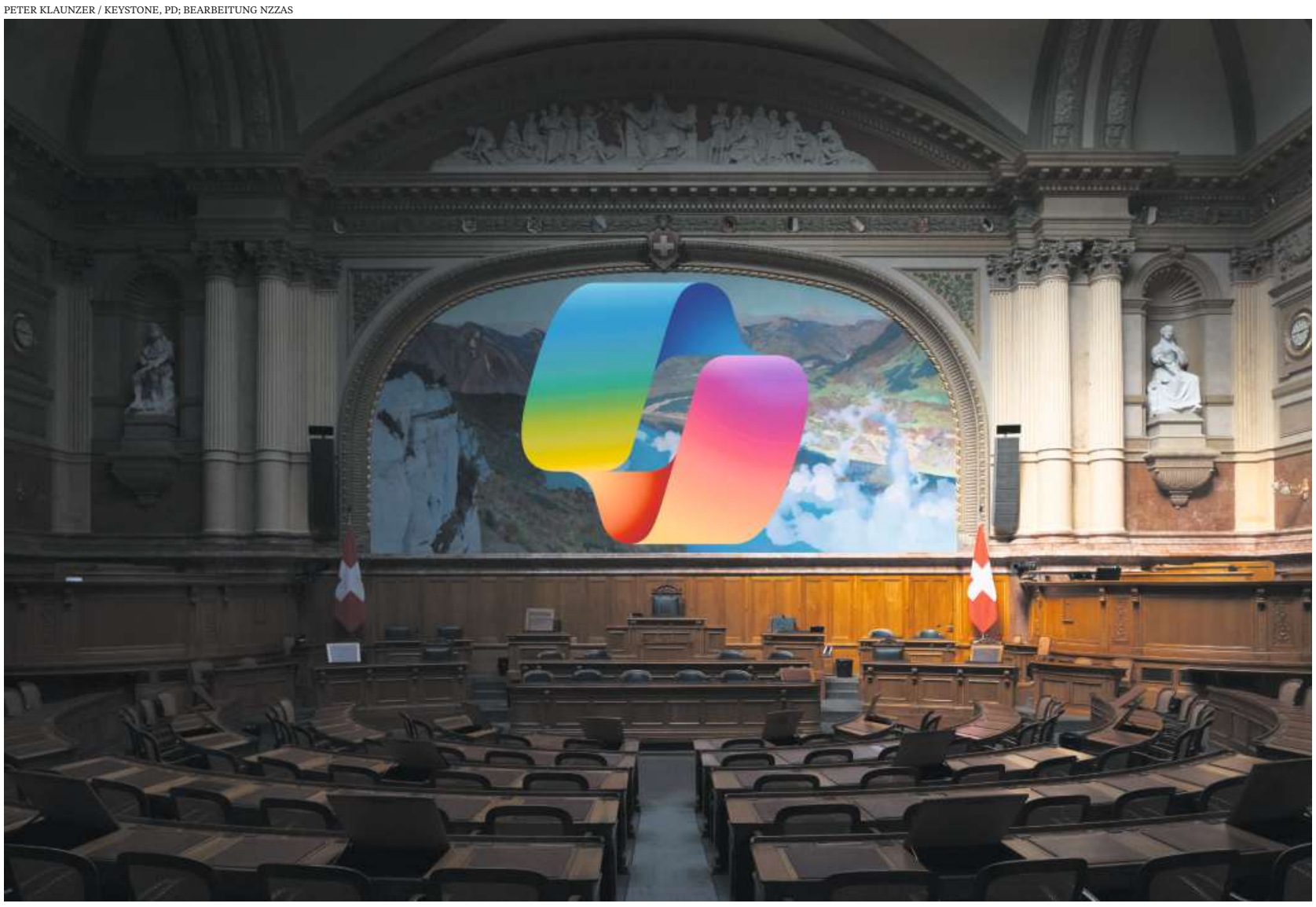
PETER KLAUNZER / KEYSTONE, PD; BEARBEITUNG NZZAS



Über allem schwebt Microsofts Copilot: Seit Mai können die Politiker im Bundeshaus ihre Dokumente mit der amerikanischen KI verarbeiten.

Datenleck im Bundeshaus

Der amerikanische Konzern Microsoft hat im Schweizer Parlament eigenmächtig künstliche Intelligenz eingeführt. Wie gross ist damit das Sicherheitsrisiko für das Land? **Von Reto Vogt**

Parlamentarier sind auch Geheimnisträger: Sie haben Einblick in geheime Papiere, ihre Kommissionssitzungen unterliegen dem Amtsgeheimnis. Vertraulichkeit ist darum ein hohes Gut unter der Bundeshauskuppel. Doch nun droht sie brüchig zu werden.

Das liegt daran, dass die künstliche Intelligenz offiziell im Bundeshaus Einzug gehalten hat. Im Mai entschied der amerikanische Konzern Microsoft, seine KI «Copilot Chat» auf den Computern der Politiker einzuführen. Seither können sie vertrauliche Dokumente wie Sitzungsprotokolle, E-Mails aus Kommissionssitzungen oder Entwürfe politischer Vorstösse mit der KI verarbeiten. Den Entscheid traf jedoch nicht die Politik, wie die Parlamentsdienste bestätigen: «Die Funktion ist Teil der Lizenz und wird von Microsoft standardmässig eingeschaltet.»

Somit hat faktisch ein amerikanischer Konzern die Einführung von künstlicher Intelligenz im Schweizer Parlament bestimmt – und damit eine heikle juristische Grauzone geschaffen. Die Tragweite dieses Vorgehens ist nicht zu unterschätzen, auch wenn es zunächst banal klingt: Copilot ist eine KI wie Chat-GPT, die Texte zusammenfassen oder Daten analysieren kann. Das Brisante daran: Laden die Politiker kritische Daten in das Tool, bewegen sie sich an der Grenze zur Amtsgeheimnisverletzung. Denn eine Garantie, dass die Daten geschützt sind, gibt es nicht.

Ganze Verwaltung betroffen

Zwar betonen die Parlamentsdienste, dass die Dokumente «in der Parlamentsumgebung bleiben und nicht zum Training der künstlichen Intelligenz verwendet werden». Doch wo die Daten konkret verarbeitet werden und ob Microsoft oder US-Behörden theoretisch Zugriff haben, bleibt offen. Klar ist nur, dass der amerikanische Konzern amerikanischem Recht unterliegt, das unter bestimmten Bedingungen den Zugriff auf Daten ermöglicht, selbst wenn diese auf Schweizer Servern liegen.

Das Parlament ist mit diesem Problem nicht allein, die ganze Bundesverwaltung ist betroffen. Microsoft aktiviert Copilot standardmässig für alle Kundinnen und Kunden, die über die entsprechende Lizenz verfügen – ohne dass diese explizit zustimmen müssen. So auch in der Bundesverwaltung, die ihre 54 000 Arbeitsplätze per Mitte Dezember auf Microsofts neuste Office-Version M365 umgerüstet hat. Die Chat-Version der KI steht allen Mitarbeitenden zur Verfügung, wie der Sprecher Klaus von Muralt bestätigt. Für deren Nutzung gelte, dass keine kritischen Daten und Inhalte eingegeben werden dürfen. Ausserdem prüfe die Bundeskanzlei, «inwiefern die integrierte Copilot-Version in Zukunft sicher und sinnvoll bei der Bundesverwaltung eingesetzt werden könnte».

Doch spezifisch für die Nutzung von Copilot wurden die Mitarbeiter nicht ausgebildet. «Es fanden keine Schulungen dazu statt», sagt von Muralt. Auch für die Politiker im Parlament gab es keine entsprechenden Angebote zur Nutzung der KI. Immerhin plant die Bundeskanzlei, solche für Verwaltungsmitarbeitende anzubieten, wie von Muralt schreibt. Die Parlamentsdienste haben auch keine zusätzlichen Richtlinien im Umgang mit Copilot vorgesehen. Das sei nicht notwendig, sagen sie. Die Bundeskanzlei erwähnt auf dieselbe Frage drei Merkblätter zur KI-Nutzung in der Bundesverwaltung. Von Muralt betont ausserdem, dass die Verantwortung für generierte Inhalte stets beim Menschen liege.

Die Politik reagiert gespalten auf die Einführung der KI. Der GLP-Nationalrat Beat Flach bemängelt, dass die Parlamentarier «bei der Aufschaltung dieser Funktion nicht nochmals darauf hingewiesen wurden, wie damit umzugehen ist». Aber schliesslich müsse man gewählte National- und Ständeräte nicht erziehen. Es liege an ihnen, die KI-Nutzung in Eigenverantwortung zu lernen, so Flach. Er hat Copilot ausprobiert und zeigt sich davon «masslos enttäuscht». Es sei eine «Zeitverschwendung».

Der Grünen-Nationalrat und IT-Unternehmer Gerhard Andrey wird grundsätzlich: Es sei die ewig gleiche Strategie von Digitalanbietern, vermeintlich kostenlose Funktionen hinzuzufügen, die Kunden nicht bestellt hätten. Sobald diese da seien, komme man nicht mehr davon los und akzeptiere später je nachdem auch zähneknirschend plötzliche Mehrkosten. «Das ist eine Methode, die man aus einem wenig rühmlichen Bereich bestens kennt», sagt Andrey. «Dass die Digitalbranche als einzige ihre Kundinnen und Kunden ‹User› nennt wie der Drogenmarkt, spricht Bände.» Der SVP-Nationalrat Franz Grüter fände es falsch, die KI-Funktion Copilot abzuschalten oder zu verbieten. Denn der Bund habe sich für diese Produkte entschieden, also gehörten regelmässige Updates wie eben Copilot dazu. Wolle man das nicht, müsse man die Grundsatzfrage über den Einsatz dieser Produkte stellen. Doch ihm fehlen die Alternativen. Die Innovationsvorsprünge der USA und Chinas gegenüber Europa und der Schweiz «sind zu gross und uneinholbar», sagt Grüter.

> Wo die Daten konkret verarbeitet werden und ob Microsoft oder die US-Behörden Zugriff haben, bleibt offen.

UBS ging schrittweise vor

Im Bereich künstlicher Intelligenz hat Grüter recht, dort hinkt die Entwicklung in Europa tatsächlich stark hinterher. Im Bereich Bürosoftware sieht es anders aus. Die Bundeskanzlei und die Stadt Zürich testen derzeit, ob die Open-Source-Lösung Open Desk dereinst Microsoft ablösen könnte. Doch selbst wer bei Microsoft bleibt, kann die Einführung von Copilot kontrollierter gestalten, als dies im Parlament geschehen ist. Seitens der Parlamentsdienste sagt eine Sprecherin zwar, dass eine «vollständige Deaktivierung nur eingeschränkt möglich ist», aber für alle Microsoft-Kunden gilt das so offenbar nicht.

Die Aktivierung ist zwar Standard, aber Organisationen können weitestgehend selbst bestimmen, wie sie Copilot einführen. Die UBS etwa ging schrittweise vor, wie die «NZZ am Sonntag» erfuhr. Zuerst war Copilot für alle Mitarbeitenden gesperrt. Dann wurde die Funktion schrittweise freigegeben: zunächst für Angestellte ohne Zugriff auf Kundendaten, später für alle – jedoch mit einem Filter, der erkennen soll, wenn Kundendaten eingegeben werden.

Eine Anfrage bei Microsoft bestätigt dies. Organisationen behielten die vollständige administrative Kontrolle über die Funktionen. Sie könnten zum Beispiel Copilot «jederzeit konfigurieren, einschränken oder deaktivieren und so die Übereinstimmung mit Governance-, Sicherheits- und Datenschutzanforderungen sicherstellen», so ein Sprecher des Konzerns. Weitere Fragen liess Microsoft unbeantwortet, zum Beispiel, ob die Aktivierung mit den Parlamentsdiensten oder dem Parlament selbst abgesprochen wurde oder warum Nutzerinnen und Nutzer sich nicht proaktiv für eine Aktivierung entscheiden müssen.

Das ist auch eine Antwort.