wissenschaftliches institut für die digitalisierung der arbeitswelt

Kommentar von Dr. Stefan Brink, 23.02.2026

Microsoft Copilot verarbeitete vertrauliche Mails

Behördliche Mails unterliegen ggf. gesetzlichen Vertraulichkeits- und Verschwiegenheitspflichten, etwa nach dem Sicherheitsüberprüfungsgesetz (SÜG) und der Verschlusssachenanweisung (VSA). Verstöße können als Straftat nach dem Strafgesetzbuch (z. B. § 353b StGB – Verletzung des Dienstgeheimnisses) geahndet werden.

Missachtet die KI solche Einstufungen („Nur für den Dienstgebrauch – NfD“ und höher), könnte sich also der Nutzer (die Sicherheitsbehörde) in Konflikt mit den gesetzlichen Vertraulichkeitsbestimmungen befinden.

Datenschutzrechtlich gesehen überschreiten die von Microsoft vorgenommenen Verarbeitungen (hier: Zusammenfassung vertraulicher E-Mails mit dem Copilot) ggf. den zwischen dem Nutzer (dem Unternehmen oder der Behörde) und Microsoft geschlossenen Vertrag über die sog. Auftragsverarbeitung (Art. 28 DS-GVO). Werden Dateien vom Nutzer als vertraulich markiert, etwa weil sie Betriebs- oder Geschäftsgeheimnisse enthalten bzw. der Verschlusssachenanweisung unterfallen, so wird dem Dienstleister Microsoft damit regelmäßig signalisiert, dass so gekennzeichnete Daten nicht zu verarbeiten sind.

Missachtet der Auftragsverarbeiter Microsoft solche Vorgaben, so kann er sich datenschutzrechtlich gesehen für die dann folgenden Verarbeitungen personenbezogener Daten nicht mehr auf den Auftrag des Verantwortlichen, also des Nutzers berufen; es liegt damit ein sogenannter Verarbeiterexzess vor, für den eine eigenständige Rechtsgrundlage nach Art. 6 DS-GVO zu suchen ist, aber regelmäßig nicht besteht. Damit liegt regelmäßig eine „Verletzung des

Schutzes personenbezogener Daten“, also „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“ (Art. 4 Nr. 12 DS-GVO) vor.

Eine solche Datenpanne ist nach Art. 33 DS-GVO für den Nutzer als (zuvor) Verantwortlichem und für Microsoft (als durch Verarbeiterexzess Verantwortlichen) bei der Aufsichtsbehörde binnen 72 Stunden meldepflichtig, sofern die Verletzung des Schutzes personenbezogener Daten nicht ausnahmsweise voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Ob dies der Fall ist, wäre im Einzelfall zu prüfen. Dies hängt insbesondere auch vom Umfang der unrechtmäßigen Verarbeitungen durch die KI und die weiteren Sicherungsmaßnahmen durch Microsoft ab.

Zudem sind nach Art. 34 DS-GVO, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen. Dies kann insbesondere bei Datenpannen von Sicherheitsbehörden der Fall sein.

u.a. Artikel im Handelsblatt

https://www.handelsblatt.com/technik/it-internet/unternehmen-copilot-verarbeitete-vertrauliche-mails-risiko-fuer-kunden/100202354.html

Dr. Stefan Brink, Gründer und Direktor des wissenschaftlichen Instituts für die Digitalisierung der Arbeitswelt wida/Berlin, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg a.D.