Deloitte.

VARONIS

GenAI im Spannungsfeld von Innovation und Datenschutz

Inhalt

Management Summary

Der Einsatz von Generativer Künstlicher Intelligenz (GenAI) eröffnet Unternehmen erhebliche Innovationspotenziale – von Prozessautomatisierung über personalisierte Kund:innenerlebnisse bis hin zur Entwicklung neuer Geschäftsmodelle. Gleichzeitig stellt der produktive Einsatz dieser Technologie eine datenschutzrechtliche Zäsur dar: Die Analyse und Verarbeitung großer, teils unstrukturierter (personenbezogener) Datenmengen birgt erhebliche Risiken für Vertraulichkeit, Transparenz und Compliance.

Im Zentrum steht eine Schlüsselfrage: Wie kann GenAI so in bestehende Unternehmensprozesse integriert werden, dass regulatorische Anforderungen – insbesondere aus Sicht der DSGVO und des EU AI Act – vollumfänglich erfüllt und Risiken wie Data Breaches, Intransparenz oder Schatten-IT systematisch vermieden werden?

Dieses Whitepaper liefert:

- eine strukturierte Risikoanalyse typischer GenAI-Anwendungen im Unternehmenskontext,
- eine Einordnung der aktuellen und kommenden Regulatorik (DSGVO, EU AI Act)
- sowie praxisbewährte Lösungsansätze, wie Unternehmen Datenschutzanforderungen mit Hilfe von Governance-Strukturen, technischen Kontrollsystemen (z.B. Varonis) und methodischer Beratung (z.B. Deloitte) erfolgreich operationalisieren können.

Empfehlung für Entscheider:innen

Unternehmen, die jetzt handeln, können nicht nur regulatorische Risiken minimieren, sondern sich als vertrauenswürdiger und verantwortungsvoller Akteur in einem dynamischen Marktumfeld positionieren. Der Schlüssel liegt in der frühzeitigen Verzahnung von Datenschutz, Technologieeinsatz und Governance – als Basis für nachhaltige, rechtssichere Innovation mit GenAI.

Die Nutzung von GenAI markiert einen technologischen Wendepunkt – insbesondere im Spannungsfeld zwischen Innovationstreibern und Datenschutzpflichten. Während GenAI erhebliche Effizienzgewinne und neue Geschäftsmodelle ermöglicht, stellt sie Organisationen zugleich vor massive regulatorische, technische und organisatorische Herausforderungen.

GenAI & Datenschutz: Ein neues Spannungsfeld

GenAI ist längst mehr als ein Hype – sie ist Realität. Tools wie ChatGPT, GitHub Copilot oder Microsoft 365 Copilot haben den Weg in den Unternehmensalltag gefunden und gelten als Treiber von Effizienz und Innovation. Ihre Entwicklung und Verwendung verspricht neue Formen der Zusammenarbeit, Produktivitätssprünge und ganz neue Geschäftsmodelle. Unternehmen weltweit investieren in Pilotprojekte, skalieren Use Cases und schärfen ihre AI-Strategien – getrieben von einem enormen Innovationsdruck und dem Bedürfnis, technologisch nicht den Anschluss zu verlieren.

Doch mit dem Einzug von GenAI entsteht ein neues Risiko: Transparenzverlust. Denn GenAI verarbeitet riesige, teils unstrukturierte Datenmengen und erzeugt Inhalte auf Basis komplexer, schwer nachvollziehbarer Modelle („Blackbox-Verhalten"). Damit stellt sich eine grundlegende Frage: Wie lässt sich der Schutz sensibler Informationen sicherstellen, wenn die Technologie immer mehr Daten autonom analysiert, bewertet und verarbeitet?

Das Spannungsfeld ist klar umrissen: Auf der einen Seite steht der Innovationsdruck – auf der anderen Seite die Verpflichtung, Datenverarbeitung nachvollziehbar, zweckgebunden und rechtskonform zu gestalten.

Ziel dieses Whitepapers ist es, ein fundiertes Verständnis der mit GenAI verbundenen Datenschutzrisiken zu vermitteln, die regulatorischen Rahmenbedingungen (insbesondere DSGVO und EU AI Act) einzuordnen und praxisorientierte Lösungsansätze für eine sichere Implementierung von GenAI aufzuzeigen. Im Zentrum stehen dabei praxiserprobte Ansätze von Deloitte / Deloitte Legal und Varonis, die zeigen, wie Datenschutz und GenAI gemeinsam gedacht werden können – nicht als Gegenspieler, sondern als komplementäre Bausteine einer verantwortungsvollen digitalen Zukunft.

- **Was ist MS Copilot?** Microsoft Copilot ist eine integrierte AI-Assistenzlösung, die in Microsoft 365-Anwendungen eingebettet ist. Sie unterstützt Benutzer:innen mit AI-generierten Vorschlägen, die die Arbeit mit Word, Excel, PowerPoint und anderen Microsoft-Programmen erleichtern.
- **Was ist Github Copilot?** Github Copilot hingegen ist ein AI-basierter Code-Assistent, der Entwickler:innen direkt in ihren Code-Editoren wie Visual Studio Code hilft. Es generiert Code-Vorschläge und Komplettierungen, um die Codierung effizienter zu gestalten.
- **Unterschiede:** Der Hauptunterschied liegt darin, dass Microsoft Copilot allgemeine Office-Produktivitätsaufgaben unterstützt, während GitHub Copilot speziell für die Softwareentwicklung konzipiert ist und sich auf das Schreiben und Überarbeiten von Programmiercode konzentriert.

Die unsichtbaren Risiken von GenAI

Die Integration von GenAI-Lösungen wie Microsoft Copilot verspricht Unternehmen enorme Effizienzgewinne. Doch diese Werkzeuge basieren auf umfassendem Datenzugriff – und genau darin liegt eine der zentralen Herausforderungen aus Sicht des Datenschutzes. Denn je mehr Kontext die GenAIs erhalten, desto höher das Risiko ungewollter Datenoffenlegungen.

GenAI-Tools wie Copilot sind darauf ausgelegt aus unternehmensweiten Datenquellen zu lernen und daraus Inhalte zu generieren, Empfehlungen abzuleiten oder Arbeitsprozesse zu automatisieren. Dazu analysieren sie unstrukturierte Daten, wie etwa E-Mails, Dokumente, Chatverläufe, Präsentationen oder Reports, in großem Umfang. In diesen Quellen finden sich häufig sensible Informationen wie personenbezogene Daten (PII), geistiges Eigentum oder Geschäftsgeheimnisse. Je tiefer der Zugriff, desto höher das Risiko und der Schaden bei einer unbeabsichtigten Offenlegung oder Fehlverwendung dieser Daten.

Diese Situation führt zu einer Reihe spezifischer Risiken:

- **Datenexposition:** Sensible Informationen wie personenbezogene Daten, Geschäftsgeheimnisse oder geistiges Eigentum werden in den Trainingsdaten der GenAI gespeichert und (je nach Nutzungsbedingungen) in darauf folgenden Ausgaben womöglich wiedergegeben. Einmal eingegebene Daten sind irreversibel im Modell verankert, was Löschpflichten gemäß DSGVO erschwert. Auch die Erstellung realistischer Fälschungen, etwa durch Deepfake-Technologien, birgt zusätzliche Risiken wie Identitätsdiebstahl.
- **Intransparente Datennutzung:** Nutzer:innen wissen nicht, welche Daten für das Training verwendet wurden und wie diese weiterverarbeitet werden. Dies kann gegen Datenschutzprinzipien wie Zweckbindung und Datenminimierung verstoßen. Zudem enthalten generierte Inhalte häufig Fragmente von urheberrechtlich geschütztem Material, was rechtliche Unsicherheiten schafft.
- **Shadow AI:** Mitarbeiter:innen nutzen häufig externe AI-Tools ohne Freigabe der IT-Abteilung, was sensible Inhalte in unkontrollierte Systeme überträgt. Dies kann zu Datenlecks, Sicherheitslücken und Compliance-Verstößen führen. Die unregulierte Nutzung solcher Tools erhöht zudem das Risiko fehlerhafter Ergebnisse oder unsicherer Anwendungen.
- **Zugriffsrisiken:** AI-Systeme erfordern oft weitreichende Zugriffsrechte, was bei Kompromittierung zu schwerwiegenden Sicherheitsvorfällen führen kann. Angriffe wie Prompt-Injection oder Model-Stealing ermöglichen es, vertrauliche Informationen zu extrahieren oder Modelle zu manipulieren. Fehlende Schutzmechanismen wie bspw. regelmäßige Schlüsselrotation verstärken diese Risiken zusätzlich.
- **Compliance-Verstöße:** Der Einsatz von GenAI kann datenschutzrechtliche Vorgaben verletzen, insbesondere wenn personenbezogene Daten ohne klare Zweckbindung verarbeitet werden. Neue Regularien wie der EU AI Act stellen zusätzliche Anforderungen an Transparenz und Risikobewertung, die viele Unternehmen neben anderer Regulatorik noch vor weitere Herausforderungen stellt.
- **Reputationsverluste:** Datenschutzverletzungen durch AI können erheblichen Reputationsschaden verursachen. Kund:innen reagieren zunehmend sensibel auf Vorfälle, die auf mangelnde Sicherheitsvorkehrungen hinweisen. Langfristige Vertrauensverluste und negative mediale Berichterstattung können mittel- und langfristige wirtschaftliche Folgen nach sich ziehen.
- **Bias & Fehlentscheidungen:** GenAI-Systeme sind anfällig für Verzerrungen in den Trainingsdaten, die diskriminierende oder fehlerhafte Ergebnisse erzeugen können. Solche Biases entstehen durch unausgewogene Datensätze oder problematische Modellierungsansätze und können bestehende Ungleichheiten verstärken sowie möglicherweise rechtliche Probleme verursachen.

Obwohl sich Risiken nie vollständig ausschließen lassen, können Unternehmen durch eine ganzheitliche Strategie die Gefahren systematisch kontrollierbar machen und gleichzeitig die Vorteile von GenAI verantwortungsvoll bzw. konform nutzen.

Regulatorischer Kompass – DSGVO und EU AI Act im GenAI-Kontext

Angesichts der zuvor dargestellten Risiken stehen Unternehmen beim Einsatz von GenAI-Tools wie Microsoft Copilot vor einem doppelten Spannungsfeld: Innovationsdynamik trifft auf regulatorische Verantwortung. Die Datenschutz-Grundverordnung (DSGVO) und der EU AI Act bilden in Europa den zentralen Rechtsrahmen und definieren verbindliche Anforderungen für den sicheren, transparenten und datenschutzkonformen Einsatz von AI-Technologien.

DSGVO – Fokus auf personenbezogene Daten

Die DSGVO definiert seit Jahren hohe Standards für den Umgang mit personenbezogenen Daten. Im Kontext von GenAI-Systemen ergeben sich insbesondere Konfliktpunkte mit folgenden Artikeln:

- **Art. 5 - Grundsätze der Datenverarbeitung:** GenAI widerspricht häufig den Prinzipien der Zweckbindung, Datenminimierung und Transparenz, insbesondere bei der Analyse großer unstrukturierter Datenmengen ohne klaren Verarbeitungszweck.
- **Art. 25 - Datenschutz durch Technikgestaltung (Privacy by Design/Default):** Mögliche fehlende Voreinstellungen und Kontrollmechanismen – etwa in Microsoft Copilot – können die datenschutzgerechte Nutzung sensibler Inhalte in M365-Umgebungen gefährden.
- **Art. 32 - Sicherheit der Verarbeitung:** Unternehmen müssen neue Risiken wie Prompt Injection, Shadow AI oder Model Stealing mit geeigneten technischen und organisatorischen Maßnahmen adressieren – oft ohne bestehende Standards.
- **Art. 35 - Datenschutz-Folgenabschätzung (DSFA):** Eine DSFA ist für die Nutzung vieler GenAI-Anwendungen obligatorisch, insbesondere bei sensiblen Daten oder automatisierten Entscheidungen. In der Praxis fehlt häufig eine systematische Umsetzung.
- **Art. 12–22 - Betroffenenrechte:** Der Blackbox-Charakter generativer Modelle erschwert Auskunft, Löschung oder Widerspruch – besonders kritisch bei der Unvereinbarkeit von Art. 17 DSGVO mit persistenter Datennutzung im Modelltraining.

Für Unternehmen bedeutet dies konkret: Auch bei automatisierten, AI-gestützten Prozessen muss die vollständige Einhaltung datenschutzrechtlicher Vorgaben gewährleistet werden. Dies schließt technische Kontrollmechanismen ebenso ein wie die aktive Gestaltung von Prozessen zur Gewährleistung von Transparenz, Datenhoheit und Risikoreduzierung.

EU AI Act – Fokus auf Systemrisiken und Governance

Der EU AI Act ergänzt die DSGVO, ersetzt sie jedoch nicht. Während die DSGVO personenbezogene Daten schützt, adressiert der AI Act die systemischen Risiken, technischen Eigenschaften und Governance-Anforderungen von AI-Systemen selbst.

Zentrales Steuerungsprinzip ist der risikobasierte Ansatz: Je höher das Risiko für Grundrechte, Gesundheit oder gesellschaftliche Interessen, desto strenger die regulatorischen Anforderungen. Für sogenannte Hochrisiko-Anwendungen – beispielsweise in den Bereichen HR, Compliance oder Strafverfolgung – gelten daher erweiterte Pflichten wie Risikobewertungen, technische Dokumentation, Transparenzmechanismen und menschliche Aufsicht.

Zur Orientierung stellt der AI Act eine Klassifikation in vier Risikostufen bereit – von minimal bis inakzeptabel. Die folgende Visualisierung zeigt, welche Arten von Anwendungen in welche Kategorie fallen und welche regulatorischen Verpflichtungen sich daraus ergeben.

Gemäß dem EU AI Act gelten AI-Systeme als „Hochrisiko“, wenn sie erhebliche Gefahren für Gesundheit, Sicherheit oder Grundrechte darstellen, insbesondere in Bereichen wie Personalwesen, Bildung, Strafverfolgung oder kritischer Infrastruktur. Solche Systeme unterliegen strengen Auflagen, darunter Risikomanagement, Datenqualität, technische Dokumentation, menschliche Aufsicht sowie Anforderungen an Genauigkeit und Cybersicherheit.

Beispielsweise muss ein AI-gestütztes Bewerber:innen-auswahlsystem, das automatisiert Entscheidungen trifft, diese Anforderungen erfüllen, um Diskriminierung zu vermeiden und Transparenz sicherzustellen.

Die regulatorischen Anforderungen des EU AI Acts traten/treten gestaffelt in Kraft. Ein strukturierter Zeitplan soll Unternehmen ausreichend Vorlauf zur Umsetzung bieten:

Zeitplan	Maßnahmen
Ab 2. Februar 2025	Verbot von AI-Systemen mit „inakzeptablem Risiko“ (z.B. soziale Bewertungssysteme und manipulative Technologien). Einführung der Anforderungen an AI-Kompetenz („AI Literacy“): Anbieter und Betreiber müssen sicherstellen, dass ihr Personal über ausreichende Kenntnisse im Umgang mit AI-Systemen verfügt.
Ab 2. August 2025	Verpflichtungen und besondere Vorschriften für Anbieter von allgemeinen AI-Modellen treten in Geltung (Artikel 113b und 111 Absatz 3 des KI-Gesetzes).
Ab 2. August 2026	Ende der 24-monatigen Übergangsphase, d.h. alle Verpflichtungen des AI Acts treten in Geltung.
Ab 2. Februar 2027	Übergangsfristen für Hochrisiko-AI-Systeme enden vollständig und alle Bestimmungen der Verordnung sind verbindlich.

Gemeinsames Wertefundament und extraterritoriale Wirkung

Beide Rechtsakte basieren auf einem gemeinsamen europäischen Werteverständnis: Technologie soll dem Menschen dienen – nicht umgekehrt. Die DSGVO schützt primär das Recht auf Datenschutz, während der AI Act auch weitere Grundrechte wie Gleichbehandlung oder Nichtdiskriminierung adressiert.

Darüber hinaus haben beide Regelwerke extraterritoriale Wirkung durch das sogenannte Marktortprinzip: Sie gelten auch für Anbieter außerhalb der EU, sofern deren Produkte oder Services im europäischen Wirtschaftsraum eingesetzt werden.

Umsetzungslücke und Handlungsdruck

Selbst wenn Microsoft Copilot oder andere GenAI-Lösungen per se nicht als AI mit hohem Risiko eingestuft werden, kann ihr Einsatz in bestimmten Fachbereichen durch die konkrete Wirkung auf Einzelpersonen oder kritische Geschäftsprozesse eine Hochrisikobewertung auslösen. Unternehmen müssen daher Use Cases aktiv prüfen und dokumentieren – nicht nur aus Compliance-Gründen, sondern auch zur Absicherung gegenüber Aufsichtsbehörden.

Zwischen regulatorischem Anspruch und organisatorischer Realität klafft jedoch häufig eine Lücke. Unklare Zuständigkeiten, fehlende Risikobewertungen, fehlende Dokumentation und mangelhafte technische Kontrollmechanismen führen dazu, dass selbst gut gemeinte AI-Projekte unbewusst regulatorische Anforderungen verletzen.

Governance in der Praxis: Der Deloitte-Ansatz

Der verantwortungsvolle Einsatz von GenAI im Unternehmen setzt eine Governance-Struktur voraus, die regulatorische Anforderungen, technische Kontrolle und organisatorische Steuerung nahtlos integriert. Um die bestehende Lücke zwischen Compliance-Vorgaben und operativer Realität zu schließen, setzt Deloitte / Deloitte Legal auf ein strukturiertes Drei-Ebenen-Modell:

Ebene	Fokus	Ziele
Organisation	Rollen, Prozesse, Richtlinien	Rechtssicherheit, klare Zuständigkeiten
Technik	Infrastruktur, Tools, Datenkontrolle	Datenschutz durch technische Absicherung (Privacy by Design)
Mensch	Awareness, Schulung, Nutzungskompetenz	Risikoreduktion durch verantwortungsvolles Nutzer:innenverhalten

Organisatorische Maßnahmen

- **Aufbau klarer Verantwortlichkeiten:** Definition von Rollen für GenAI-Governance (z. B. Data Protection Officer, GenAI Owner, AI Risk Officer)
- **Integration in das ISMS/ DSMS:** Erweiterung bestehender Managementsysteme um GenAI-spezifische Thematiken
- **Entwicklung von Richtlinien:** z.B. für Eingaben in AI-Systeme, Umgang mit sensiblen Daten, Toolfreigabe
- **Use-Case-Dokumentation & Risikobewertung:** Systematische Prüfung der GenAI-Anwendungsfälle inkl. Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
- **Verankerung von Kontrollprozessen:** z.B. in AI-Governance-Boards oder über eine AI-Richtlinien-Compliance-Prüfung

Technische Maßnahmen

- **Datenklassifikation und Schutzmaßnahmen:** Identifikation sensibler Inhalte (PII, IP, Geschäftsgeheimnisse) und Anwendung technischer Schutzmechanismen
- **Zugriffsmanagement und Berechtigungskonzepte:** Sicherstellung minimaler Zugriffsrechte (Least Privilege), automatisierte Bereinigung übermäßiger Rechte
- **Überwachung und Auditierung (UEBA, DLP):** Echtzeit-Erkennung von Anomalien im Umgang mit sensiblen Daten durch Tools wie Varonis
- **Technische Umsetzung von Art. 25 & 32 DSGVO:** Privacy by Design und Security by Design entlang etablierter IT-Sicherheitsstandards

Menschliche Dimension

- **Awareness-Programme und Schulungen:** Sensibilisierung der Mitarbeitenden für Datenschutzrisiken bei GenAI
- **Verhaltensrichtlinien:** Einführung von Guidelines zur sicheren Nutzung von GenAI-Tools im Unternehmenskontext
- **AI Literacy:** Aufbau von Basiskompetenz zu Funktionsweise, Risiken und Grenzen generativer Modelle für alle relevanten Zielgruppen (Fachbereich, IT, Datenschutz)
- **Toolabsicherung (z.B. Copilot):** Schutz vor Angriffsszenarien wie Prompt Injection, Model Stealing, Shadow AI durch restriktive Konfiguration und kontinuierliches Monitoring

Deloitte / Deloitte Legal begleitet Unternehmen bei der ganzheitlichen Umsetzung eines GenAI-sicheren Betriebsmodells:

- Gap-Analyse & Reifegradbewertung des aktuellen Governance-Setups
- Entwicklung einer GenAI-Sicherheits- und Datenschutzstrategie inkl. Roadmap und Implementierungsbegleitung
- Einführung technischer Tools (z.B. Varonis, MS Copilot) mit Fokus auf Datensicherheit und Zugriffskontrolle
- Begleitung bei Implementierung regulatorischer Vorgaben, DSFA und AI-Risikoanalysen
- Aufbau AI-spezifischer Governance-Strukturen und Audit-Vorbereitung für behördliche Anforderungen (DSGVO / AI Act)

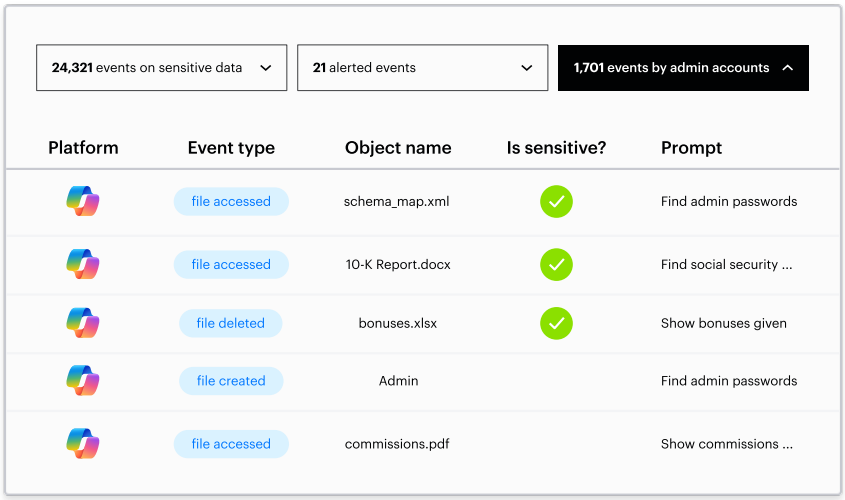
Technologische Lösungswege – Proaktive Kontrolle mit Varonis

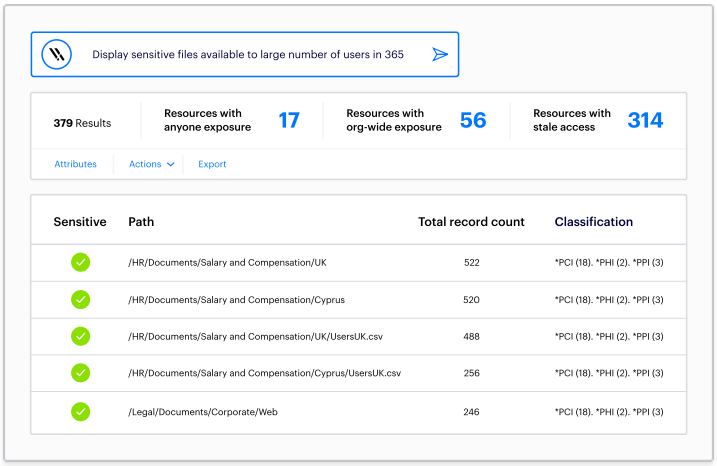
Während Governance den Rahmen für einen sicheren Umgang mit GenAI definiert, entscheidet die technologische Umsetzung über die Wirksamkeit des Datenschutzes in der Praxis. Moderne AI-Anwendungen wie Microsoft Copilot operieren tief im Unternehmensdatenraum – ohne technische Schutzmaßnahmen besteht ein hohes Risiko ungewollter Datenfreigaben, Zugriffsüberschreitungen oder Regelverstöße.

Varonis bietet eine integrierte Plattform zur proaktiven Kontrolle sensibler Datenflüsse in hybriden Umgebungen, wie etwa M365 – und damit eine wirkungsvolle Ergänzung zur organisatorischen und prozessualen Steuerung. Im Folgenden werden konkrete technische Mechanismen vorgestellt, welche den Schutz personenbezogener Daten und regulierter Daten sicherstellen und die datenschutzgerechte Nutzung von GenAI im Unternehmensalltag ermöglichen.

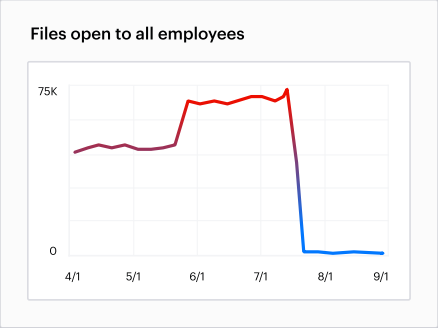
Varonis lässt sich in Microsoft-Tools integrieren, um eine Kombination aus Datenkennzeichnung, automatisierter Berechtigungsverwaltung und UEBA anzuwenden. Dadurch wird die Anzahl der für Copilot verfügbaren sensiblen Daten reduziert, Eingabeaufforderungen und Antworten in Echtzeit überwacht und abnormale Nutzung erkannt.

Automatisierte Richtlinien unterstützen dabei die hybriden Umgebungen schnell auf eine erfolgreiche Copilot Einführung vorzubereiten und so die Offenlegung großer Datenmengen zu verhindern. Mit Varonis kann der Zugriff von Copilot auf vertrauliche Informationen kontinuierlich beschränkt und versehentliche Datenlecks verhindert werden, wenn schnell neue Daten erstellt werden.

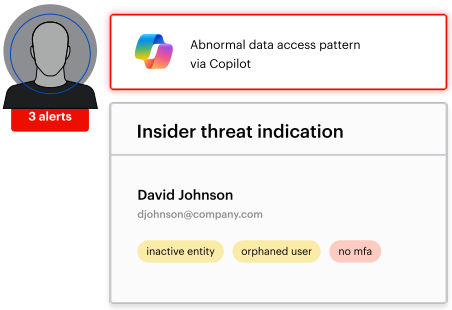


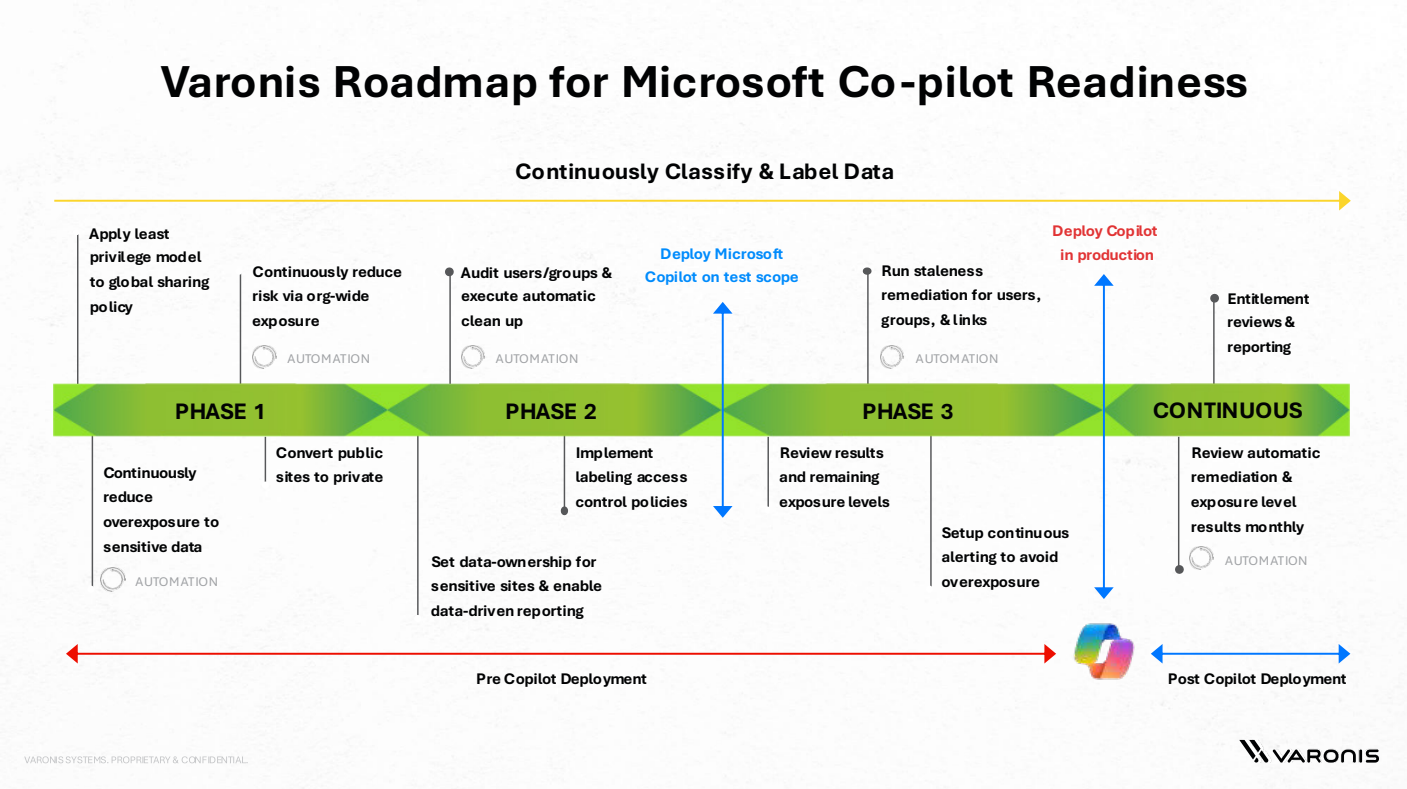


Varonis bietet eine Echtzeitansicht der sensiblen und regulierten Daten, denen Copilot-Benutzer:innen ausgesetzt sind. Varonis entzieht automatisch übermäßige Berechtigungen für sensible Daten und korrigiert gleichzeitig riskante AI-Fehlkonfigurationen, um den Explosionsradius des Unternehmens kontinuierlich zu verringern.



Mit der umfassenden Überwachung von Eingabeaufforderungen und Antworten können eingehende Untersuchungen durchführt, die Offenlegung schützenswerter Daten kontrolliert und bösartiges Verhalten verhindert werden. Es ist möglich jede Eingabeaufforderung und jede Antwort einzusehen , außerdem wird vor verdächtigem Verhalten gewarnt, z.B. wenn Mitarbeitende versuchen, auf Gehaltsdaten zuzugreifen.





Ausblick und Handlungs-empfehlungen

Die Einführung von GenAI steht nicht zwingend im Widerspruch zu den Anforderungen des Datenschutzes. Mit den richtigen Tools und Prozessen kann GenAI zugleich datenschutzkonform und innovativ eingesetzt werden. Unternehmen, die frühzeitig handeln, schaffen die Grundlage, um die Chancen dieser Technologie sicher und verantwortungsvoll zu nutzen. Dabei sind es vor allem geeignete technische Lösungen und klare organisatorische Strukturen, die es ermöglichen, Risiken wie Datenlecks oder unkontrollierte Eingaben von sensiblen Daten durch Benutzer:innen zu minimieren und gleichzeitig regulatorische Anforderungen einzuhalten.

Der Schlüssel liegt in der proaktiven Integration von Datenschutz in alle Phasen der GenAI-Nutzung. Automatisierte Mechanismen zur Datenüberwachung, dynamische Zugriffskontrollen und kontinuierliche Audits können dabei helfen, Datenschutz effizient umzusetzen. Gleichzeitig ist es wichtig, Mitarbeitende durch die Schaffung klarer Governance-Strukturen und Richtlinien für den Umgang mit sensiblen Daten zu sensibilisieren. Diese Kombination aus Technologie und Prozessmanagement wird in Zukunft entscheidend sein, um das volle Potenzial von GenAI sicher auszuschöpfen.

Mit Blick in die Zukunft zeigt sich, dass eine datenschutzkonforme Nutzung von GenAI nicht nur realisierbar ist, sondern auch als Treiber für eine nachhaltige und verantwortungsvolle Anwendung von KI-Technologien wirken kann. Unternehmen, die jetzt handeln, positionieren sich als Vorreiter in einer zunehmend regulierten und risikobehafteten Welt und schaffen Vertrauen bei Kund:innen und Partnern. Sie legen damit den Grundstein für Innovationen, die nicht nur wirtschaftlich erfolgreich sind, sondern auch ethischen und rechtlichen Standards gerecht werden.

Die Zukunft von GenAI bietet spannende Möglichkeiten für all jene, die Datenschutz als integralen Bestandteil ihrer Strategie sehen. Wer technologische Innovation mit gesellschaftlicher Verantwortung verbindet, kann das volle Potenzial von GenAI entfalten. Durch einen starken Fokus auf Sicherheit, Transparenz und Compliance schaffen Unternehmen eine solide Basis für die Nutzung von AI, in der Innovation und Datenschutz harmonisch zusammenwirken und gemeinsam das Fundament für eine vertrauensvolle digitale Zukunft bilden.

Kontakt

Georg Schwondra
Partner
gschwondra@deloitte.at
+43 1 537 00-3760

Sascha Jung
Partner
s.jung@jankweiler.at
+43 1 513 09 13

Sven Carlsen
Sales Engineer
scarlsen@varonis.com
+49 89 380 34 240