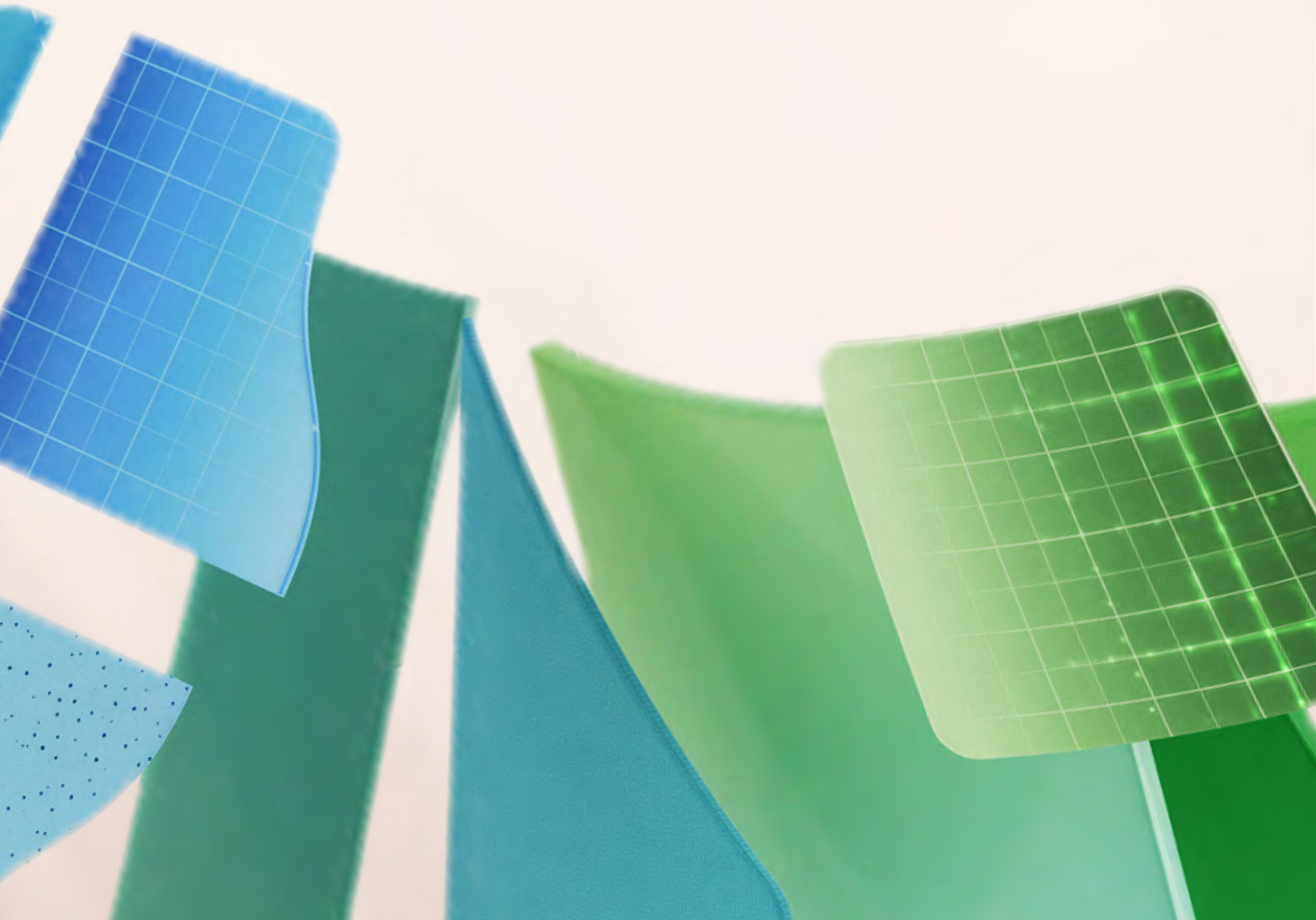
Microsoft 365

Daten auf dem Prüfstand

Optimierte Data Governance für eine erfolgreiche KI-Einführung



Inhaltsverzeichnis

Überblick

Data Governance ist das Rückgrat der sicheren KI-Einführung

Generative KI verspricht Unternehmenstransformationen – doch die Nutzung dieses Potenzials hängt von der Qualität und Verfügbarkeit Ihrer Geschäftsdaten ab.

Unternehmen, die eine starke Data Governance priorisieren, sind bestens aufgestellt, um sich mit KI einen Wettbewerbsvorteil zu verschaffen. Data Governance trägt dazu bei, dass Daten, die von KI abgefragt und generiert werden, korrekt und sicher sind, kontrolliert werden und den Vorschriften entsprechen.

Datenqualität und -verfügbarkeit: KI-Systeme sind auf große, qualitativ hochwertige Datensätze angewiesen, um die bestmögliche Antwort mit dem richtigen Kontext aus den individuellen Workflows Ihres Unternehmens bereitzustellen. Eine bessere Datenqualität führt zu effektiveren KI-Insights und -Vorhersagen.

Compliance: Eine starke Data Governance gewährleistet die Einhaltung gesetzlicher Anforderungen und reduziert das Risiko von rechtlichen Problemen und Bußgeldern.

Sicherheit: Die ordnungsgemäße Kennzeichnung und Verwaltung von Daten schützt vertrauliche Informationen vor nicht autorisiertem Zugriff, unbefugter Weitergabe und Datenschutzverletzungen.

Vertrauen: Zuverlässige Data Governance stärkt das Vertrauen der Stakeholder in die KI-Ergebnisse und fördert so eine stärkere Akzeptanz und Unterstützung für KI-Initiativen.

In diesem E-Book werden wichtige Data Governance-Praktiken vorgestellt, die ein KI-bereites Unternehmen ausmachen. Es umfasst die Einrichtung robuster Datenqualitätsstandards, die Sicherstellung der Einhaltung regulatorischer Anforderungen sowie die Implementierung von Datenschutz- und Sicherheitsmaßnahmen. Ganz gleich, ob es darum geht, vertrauliche Meetinginhalte vor externer Freigabe zu schützen oder sich vor Datenschutzverletzungen zu schützen: Sie lernen Strategien kennen, mit denen Sie Vertrauen in KI-Systeme schaffen und Daten leicht verfügbar machen können, um verwertbare Insights zu gewinnen. Durch die Einführung dieser Praktiken kann Ihr Unternehmen das volle Potenzial von KI für kontinuierliche Innovation und Wettbewerbsvorteile nutzen.

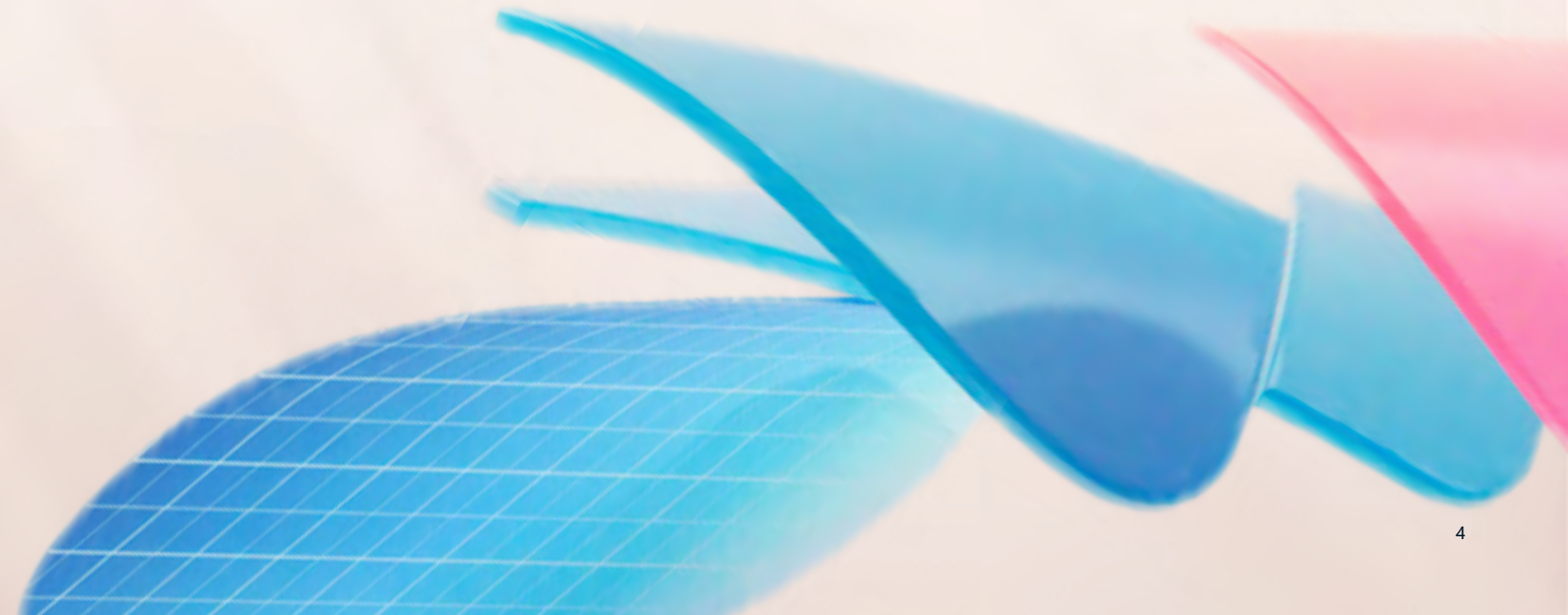
Anwendungsfälle für generative KI

Beschleunigen der Kommunikation: Entwerfen Sie personalisierte Inhalte schneller, und gewinnen Sie Zeit für den Aufbau von Beziehungen und die Zusammenarbeit.

Verbessern der Effizienz: Reduzieren Sie den Zeitaufwand für Routineaufgaben, steigern Sie die Produktivität und senken Sie Kosten.

Ermöglichen von Innovationen: Entwickeln Sie Ideen und Vorschläge für neue Produkte und Dienste.

Personalisieren von Customer Experiences: Passen Sie Inhalte und Empfehlungen an, um Kundenbindung und -interaktion zu fördern.



1

Stärkung der Data Governance für die KI-Transformation

Jedes Unternehmen verfügt über Richtlinien und Prozesse, die die Datennutzung regeln. Data Governance-Frameworks variieren in Reifegrad und Umfang, aber nur wenige wurden vollständig für KI optimiert. Während viele bewährte Data Governance-Methoden unverändert bleiben, z. B. die Gewährleistung der Datengenauigkeit und -konsistenz, müssen andere Aspekte aktualisiert werden, um die Investitionen in KI zu maximieren. Sehen wir uns einige wichtige Bereiche an.

Datentransparenz

Detaillierte Kenntnisse des Datenflusses innerhalb von KI-Systemen ermöglichen es, eine unbefugte oder unangemessene Nutzung zu erkennen und zu unterbinden. Diese Transparenz trägt zur Unterstützung von Sicherheit und Compliance bei, indem vertrauliche Daten geschützt werden, um den Wert von KI zu maximieren.

Herkömmliche Data Governance konzentrierte sich darauf, zu wissen, wo sich Daten befinden, und den Zugriff zu kontrollieren. Mit der zunehmenden Integration von KI in die Geschäftsabläufe muss Data Governance jedoch mit neuen Sicherheitsanforderungen Schritt halten.

Bei einer hochsensiblen Produkteinführung muss sich die Governance nun auch auf die Verwaltung von KI-generierten Inhalten erstrecken, um sicherzustellen, dass die von KI erzeugten projektbezogenen Dokumente, Mitteilungen und Insights sicher sind. Dazu müssen Sicherheitsmaßnahmen implementiert werden, damit nur autorisierte Teammitglieder auf KI zugreifen und diese nutzen können, um Projektinformationen zu analysieren oder zusammenzufassen.

Darüber hinaus können Unternehmen durch die Verwaltung von Datenverarbeitungs- und Speichervolumen die mit KI verbundenen Betriebskosten besser kontrollieren.

Datenqualität

KI verstärkt die Wichtigkeit hochwertiger Daten, da sich eine schlechte Datenqualität direkt auf die KI-Ergebnisse auswirkt. Wenn Sie KI-Tools zur Abfrage Ihrer Geschäftsdaten einsetzen, möchten Sie sicherstellen, dass die Daten aktuell und vertrauenswürdig sind. Ebenso wichtig ist es, die Herkunft und Qualität der Daten zu verstehen, die Ihre Teams verwenden, um ihre eigenen KI-Modelle und Apps zu entwickeln. Regelmäßige Datenaudits, strenge Validierungsprozesse und eine proaktive Verwaltung tragen dazu bei, die Datenintegrität sicherzustellen. Durch die Fokussierung auf diese Bereiche können Unternehmen zuverlässige KI-Ergebnisse erzielen, die die Entscheidungsfindung verbessern und Innovationen vorantreiben.

Benutzerverwaltung

Mit KI interagieren Benutzende auf raffinierte Weise mit Daten. Sie kommunizieren mit KI-Systemen wie Microsoft 365 Copilot über Prompts in natürlicher Sprache. Sind Berechtigungen und Schutzmaßnahmen vorhanden, kann KI auf relevanten Kontext aus Daten wie Dateien, Chats und E-Mails sowie über Plug-ins auch auf externe Quellen zugreifen, um eine Antwort zu generieren.

Es ist wichtig, die in diesen Prozessen verwendeten Daten zu überwachen, um sicherzustellen, dass KI korrekte, fundierte Antworten liefert. Transparenz durch Fußnoten oder Links zu Originalquellen hilft Benutzenden, die Informationen zu überprüfen, wodurch das Risiko von Datenmissbrauch verringert und die Einhaltung von Vorschriften sichergestellt wird.

Compliance und eDiscovery

Der zunehmende Einsatz von KI bringt neue Herausforderungen in Bezug auf Compliance und eDiscovery (Verarbeitung von Daten für Rechtsfälle) mit sich, insbesondere bei der Verwaltung von KI-generierten Daten und bei der Anpassung an neue gesetzliche Anforderungen. Die Aktualisierung von Data Governance-Frameworks, um diesen Herausforderungen zu begegnen, erfordert die Entwicklung von Richtlinien, die KI-generierte Inhalte abdecken und beispielsweise sicherstellen, dass von KI erstellte Dokumente oder Mitteilungen sicher nachverfolgt, kategorisiert und gespeichert werden. Beispielsweise müssen Richtlinien möglicherweise aktualisiert werden, um sicherzustellen, dass KI-generierte E-Mails oder Berichte ordnungsgemäß markiert und für einen späteren Abruf archiviert werden.

Die Verbesserung der eDiscovery-Funktionen würde die Integration von KI-Tools umfassen, die KI-generierte Inhalte auf verschiedenen Plattformen suchen und identifizieren können. Bei einer Rechtsanfrage müssen eDiscovery-Tools beispielsweise in der Lage sein, bestimmte KI-generierte Dokumente zu finden und abzurufen, relevante Mitteilungen zusammenzufassen und klare Prüfpfade bereitzustellen, um die Einhaltung der Vorschriften nachzuweisen. Durch die Aktualisierung dieser Funktionen können Unternehmen Daten bei rechtlichen Prüfungen oder Ermittlungen besser verwalten und sicherstellen, dass alle relevanten KI-generierten Informationen zugänglich und vor Gericht vertretbar sind.

Datensicherheit

Der Schutz KI-gesteuerter Abläufe sollte Zero-Trust-Prinzipien auf Identitätsebene beinhalten, um das Risiko unbefugter Zugriffe zu minimieren. Regelmäßige Updates an Endpunkten, einschließlich Geräten und Anwendungen, reduzieren Schwachstellen, die ausgenutzt werden könnten. Die im Unternehmen verwendeten Tools für generative KI zu kennen, ermöglicht es, nicht genehmigte oder unsichere Anwendungen zu blockieren, was wiederum potenzielle Sicherheitsverletzungen verhindert. Durch die Beschränkung des Zugriffs auf KI-Tools und -Daten auf vertrauenswürdige Mitarbeitende können Unternehmen eine höhere Datenintegrität erreichen und ihre KI-Prozessen vor potenziellen Bedrohungen schützen.

Was ist Zero Trust?

Zero Trust ist ein Sicherheitsmodell, das jede Anfrage so verifiziert, als käme sie aus einem nicht vertrauenswürdigen Netzwerk. Anstatt davon auszugehen, dass alles innerhalb der Unternehmensfirewall sicher ist, folgt dieser Ansatz dem Prinzip „niemals vertrauen, immer überprüfen“.

Zero-Trust-Prinzipien

Explizit überprüfen: Authentifizierung und Autorisierung müssen immer basierend auf allen verfügbaren Datenpunkten ausgeführt werden.

Zugriff mit geringstmöglichen Berechtigungen: Beschränken Sie den Benutzerzugriff mit Just-in-Time- und Just-Enough-Access-Prinzipien (JIT/JEA), risikobasierten adaptiven Richtlinien und Datenschutzfunktionen.

Annahme einer Sicherheitsverletzung: Begrenzen Sie Schäden, kontrollieren Sie den Zugriff, stellen Sie Verschlüsselung sicher, und nutzen Sie Daten, um Bedrohungen zu erkennen und Abwehrmaßnahmen zu stärken.

2

Die Rolle von Datenverantwortung bei der KI-Transformation: Ursprung, Qualität und Zuverlässigkeit

Wenn Unternehmen KI zur Unterstützung von Geschäftsentscheidungen einsetzen, müssen sie sicherstellen, dass diese Systeme korrekte und zuverlässige Ergebnisse liefern können. Die Datengrundlagen, auf denen die KI-Antworten basieren, müssen verfügbar, konsistent und gut dokumentiert sein.

Datenverantwortung unterstützt vertrauenswürdige KI durch die Implementierung von Governance-Richtlinien, die nachverfolgen, woher Daten stammen, ihre Qualität überprüfen und ihre Zuverlässigkeit und Genauigkeit sicherstellen. Diese Praktiken bilden die Grundlage für KI-Systeme, die zuverlässige Insights liefern und so fundierte und vertrauensvolle Entscheidungen ermöglichen.

Datenherkunft: Ursprünge und Veränderungen von Informationen verstehen

Datenherkunft verfolgt den Weg von Daten durch ein Unternehmen. Sie dokumentiert den Ursprung, die Transformationen und die Ziele der Daten. Für KI-gestützte Unternehmen ist das Verständnis der Datenherkunft aus verschiedenen Gründen wichtig:

- **Transparenz:** Zu wissen, woher Daten stammen und wie sie sich verändern, hilft dabei, die Genauigkeit von KI-generierten Ausgaben zu bestätigen, und stellt durch ein klares Verständnis der Datenhistorie regulatorische Compliance sicher.
- **Rückverfolgbarkeit:** Datenherkunft ermöglicht Unternehmen, Fehler oder Inkonsistenzen bis zu ihren Quellen zurückzuverfolgen, was die Problembehandlung und Datenkorrektur vereinfacht.
- **Auswirkungsanalyse:** Wenn Sie verstehen, wie Daten von Tools für generative KI verwendet werden, können Sie die potenziellen Auswirkungen von Änderungen an Datenquellen oder Verarbeitungsmethoden auf die Ausgabegenauigkeit und die Geschäftsergebnisse bewerten.

Datenqualität: Qualität steigert den Wert von KI-Antworten.

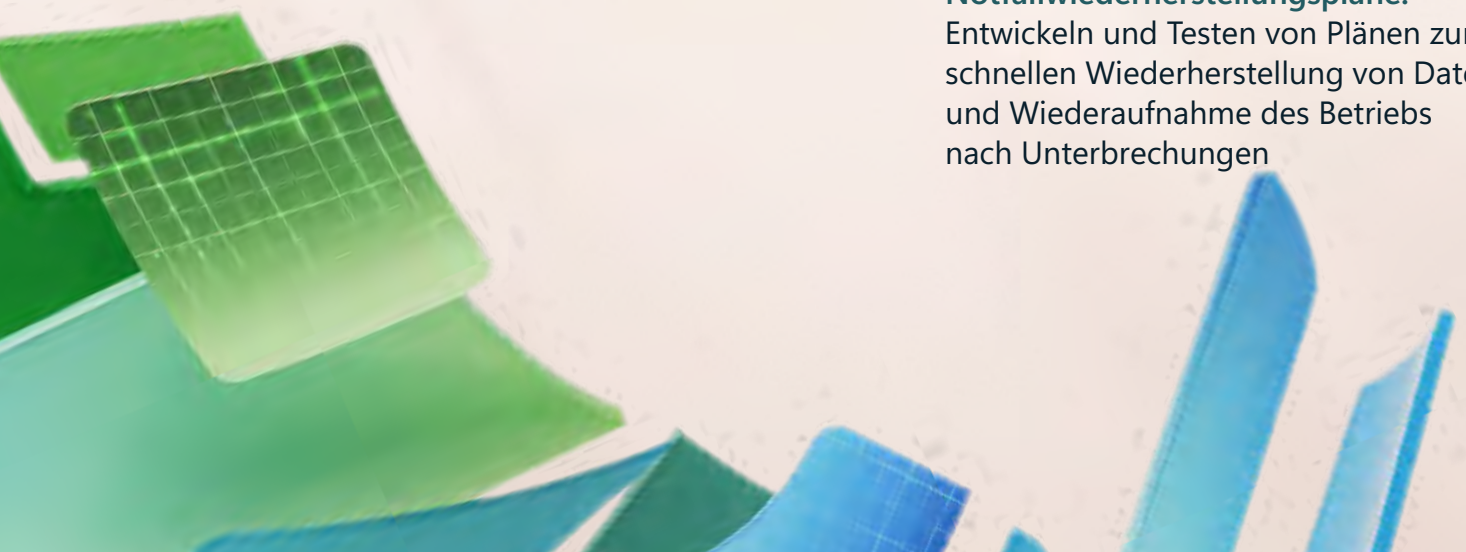
Datenqualität wirkt sich direkt auf die Zuverlässigkeit von KI-Ausgaben aus. Qualitativ hochwertige Daten liefern den Kontext, damit KI-Modelle korrekte und wertvolle Antworten auf Benutzereingaben liefern können. Zu den wichtigsten Aspekten der Datenqualität zählen:

- **Genauigkeit:** Die Daten müssen die realen Bedingungen korrekt darstellen.
- **Vollständigkeit:** Alle notwendigen Daten müssen vorhanden sein und berücksichtigt werden.
- **Konsistenz:** Die Daten müssen über verschiedene Systeme hinweg und im Laufe der Zeit konsistent sein.
- **Aktualität:** Die Daten müssen aktuell und bei Bedarf immer verfügbar sein.

Datenzuverlässigkeit: Sicherstellung von vertrauenswürdigen Daten

Datenzuverlässigkeit bedeutet, dass Daten stets den Qualitätsstandards entsprechen und bei Bedarf immer verfügbar sind. Für KI-gestützte Unternehmen sind zuverlässige Daten entscheidend, um das Vertrauen in KI-Tools und die Entscheidungen, die auf diesen basieren, zu fördern. Die Sicherstellung der Datenzuverlässigkeit umfasst:

- **Datenredundanz:** Implementieren von Sicherungssystemen, die Datenverlust verhindern und die Verfügbarkeit erhöhen
- **Regelmäßige Sicherungen:** Durchführen häufiger Sicherungen, um Daten vor Beschädigung oder Verlust zu schützen
- **Überwachung und Warnhinweise:** Einrichten von Überwachungssystemen zur Erkennung von Datenproblemen und zur Benachrichtigung aller Beteiligten in Echtzeit
- **Notfallwiederherstellungspläne:** Entwickeln und Testen von Plänen zur schnellen Wiederherstellung von Daten und Wiederaufnahme des Betriebs nach Unterbrechungen



3

Die Beziehung zwischen Governance, Sicherheit und verantwortungsvoller KI

Zusammen bilden Data Governance und Sicherheit das Rückgrat für einen verantwortungsvollen Einsatz von KI. Hochwertige, sichere Daten gewährleisten, dass KI ethisch und effektiv arbeitet. Zu den wichtigsten Bereichen, die bewertet werden müssen, gehören Datenklassifizierung, Zugriffskontrollen, Verschlüsselung, Reaktion auf Vorfälle und regulatorische Compliance.

Datenklassifizierung

Das Klassifizieren von Daten ist ein wichtiger Teil der Kontrolle des Umgangs von KI-Tools mit vertraulichen Informationen. In der Regel werden Daten und Meetings als allgemein, vertraulich oder streng vertraulich eingestuft. Die richtige Klassifizierung stellt sicher, dass KI nur auf die benötigten Informationen zugreift, und verringert so das Risiko, dass vertrauliche Daten für unbefugte Benutzende offengelegt werden.

Eine falsche Klassifizierung hingegen kann dazu führen, dass KI Daten verarbeitet, die nur eingeschränkt verfügbar sein sollten, was zu Sicherheitsverletzungen oder Compliance-Problemen führt. Eine effektive Data Governance, sei es durch automatisierte Tools oder Anwenderrichtlinien, stellt sicher, dass Daten korrekt klassifiziert werden, schützt vertrauliche Informationen und unterstützt die Fähigkeit von KI, zuverlässige und konforme Ergebnisse zu liefern.

Zugriffskontrollen

Diese Kontrollen regeln, wer auf KI-relevante Daten zugreifen kann und welche Anwendungen oder Identitäten die Berechtigung zur Interaktion mit diesen Daten haben. Schwache Zugriffskontrollen können zu nicht autorisierter Offenlegung vertraulicher Informationen führen, was das Risiko von Sicherheitsverletzungen und Missbrauch erhöht.

Data Governance spielt eine Schlüsselrolle bei der Durchsetzung dieser Kontrollen: Sie beschränkt den Datenzugriff auf autorisiertes Personal und bestimmte Anwendungen und stellt so sicher, dass vertrauliche Daten angemessen verarbeitet werden. Dies schützt nicht nur die Datenintegrität, sondern gewährleistet auch, dass KI-Systeme mit sicheren, vertrauenswürdigen Datensätzen arbeiten, was ihre Zuverlässigkeit und Compliance verbessert.

Verschlüsselung

Der Schutz von Daten vor Abfangen und Manipulation durch Verschlüsselung trägt dazu bei, dass Tools für generative KI ihre Antworten im richtigen Kontext – z. B. arbeitsbezogene Daten, Dateien, Chats und E-Mails – erstellen können, ohne Datenverluste zu riskieren.

Data Governance-Richtlinien können robuste Verschlüsselungspraktiken vorschreiben, die Daten während ihres gesamten Lebenszyklus schützen. Dieser Ansatz stellt sicher, dass KI-Tools zuverlässige Antworten liefern können. Gleichzeitig werden Ihre Daten geschützt und das Vertrauen wird aufrechterhalten.

Reaktion auf Vorfälle

Vertrauliche Unternehmensdaten können durch Vorfälle mit Tools für generative KI offengelegt werden, die nicht autorisierten Zugriff auf Dateien, E-Mails oder andere Geschäftsdaten gewähren, welche Systeme zum Generieren von Antworten verwenden.

Ein proaktiver Plan für die Reaktion auf Vorfälle ist in diesen Szenarien entscheidend. Ohne einen solchen Plan riskieren Unternehmen nicht nur die Offenlegung vertraulicher Daten, sondern auch kompromittierte Ausgaben der KI. Data Governance umfasst detaillierte Reaktionsprotokolle, um schnell auf Sicherheitsverletzungen zu reagieren, ihre Auswirkungen zu minimieren und die Zuverlässigkeit von KI-Systemen zu erhalten.

Regulatorische Compliance

KI-Anwendungen müssen Vorschriften wie der DSGVO oder dem CCPA entsprechen, die den Datenschutz und Privatsphäre regeln. Eine Nichteinhaltung dieser Vorschriften kann zu erheblichen Sanktionen führen und das Vertrauen untergraben. Es ist auch wichtig zu verstehen, wo KI-Tools Daten verarbeiten, da viele kostenlose Tools Daten ggf. global oder außerhalb der üblichen Speicherorte Ihres Unternehmens verarbeiten. Data Governance stellt sicher, dass KI-Anwendungen nicht nur innerhalb der gesetzlichen Rahmenbedingungen ausgeführt werden, sondern dass sich die Daten auch innerhalb der richtigen Dienstgrenzen befinden und den Compliance-Standards Ihres Unternehmens entsprechen. Dieser Ansatz unterstützt die ethische Nutzung von KI und hilft, Vertrauen in die KI-Technologie aufzubauen.

4

Aktualisieren Ihres Data Governance-Frameworks zur Unterstützung der KI-Einführung

In der sich entwickelnden KI-Landschaft ist es wichtig, spezifische Bereiche Ihres bestehenden Data Governance-Frameworks zu identifizieren, die besondere Aufmerksamkeit erfordern könnten. Anstatt das gesamte Framework zu überarbeiten, können Sie sich auf Bereiche konzentrieren, die sich am ehesten weiterentwickeln werden. Konzentrieren Sie Ihre Aktivitäten auf die Bereiche, in denen sie den Wert von KI am meisten steigern, und stellen Sie gleichzeitig sicher, dass Ihre Daten geschützt und abgesichert bleiben. Hier einige wichtige Insights, die es zu berücksichtigen gilt:

Anpassen von Richtlinien und Verfahren

KI erfordert neue Arten der Datenerfassung, -verarbeitung und -nutzung. Die Aktualisierung von Datenrichtlinien kann dazu beitragen, relevante Anforderungen in Bezug auf Datenschutz, regulatorische Compliance und ethische Nutzung zu erfüllen. Beispielsweise kann das Erfordern von Datenanonymisierung in bestimmten Fällen personenbezogene Daten schützen, wodurch ihre Verwendung während des gesamten KI-Lebenszyklus sicherer wird.

Rollen und Verantwortlichkeiten

Es ist von entscheidender Bedeutung, KI-Readiness für alle mit Data Governance verbundenen Rollen zu gewährleisten. Mitarbeitende, die mit den KI-Datenanforderungen vertraut sind, können als Data Stewards fungieren, um die Datenqualität und Compliance zu unterstützen. Die funktionsübergreifende Zusammenarbeit zwischen Rechts-, IT- und Data Science-Teams kann dazu beitragen, KI-spezifische Herausforderungen effektiver anzugehen.

Anpassen von Datenstandards und -definitionen

Indem Datenformate, Definitionen und Qualitätskennzahlen standardisiert werden, wird die Implementierung von Richtlinien für die Nutzung von KI-Tools innerhalb eines Unternehmens vereinfacht. Klare Datenstandards erleichtern die Entscheidung, welche Datensätze KI-Tools nutzen können, um Geschäftskontext bereitzustellen, und welche Daten Benutzende zur Analyse hochladen können. Dadurch wird sichergestellt, dass KI-Anwendungen die relevantesten und vertrauenswürdigsten Daten verwenden, was ihre Effektivität steigert und gleichzeitig die Einhaltung der Unternehmensrichtlinien unterstützt.

Kontinuierliche Verbesserung

Data Governance ist ein fortlaufender Prozess, insbesondere bei KI. Regelmäßige Audits und Aktualisierungen Ihres Governance-Frameworks können Ihnen dabei helfen, es an neue KI-Entwicklungen und regulatorische Änderungen anzupassen. KI selbst kann verwendet werden, um Governance-Praktiken zu überprüfen und zu verbessern, um möglicherweise Lücken zu finden und Verbesserungen vorzuschlagen. Dieser proaktive Ansatz verbessert die Compliance und Effizienz im Zuge der Weiterentwicklung von KI-Technologien.

Tools und Techniken für eine effektive Data Governance

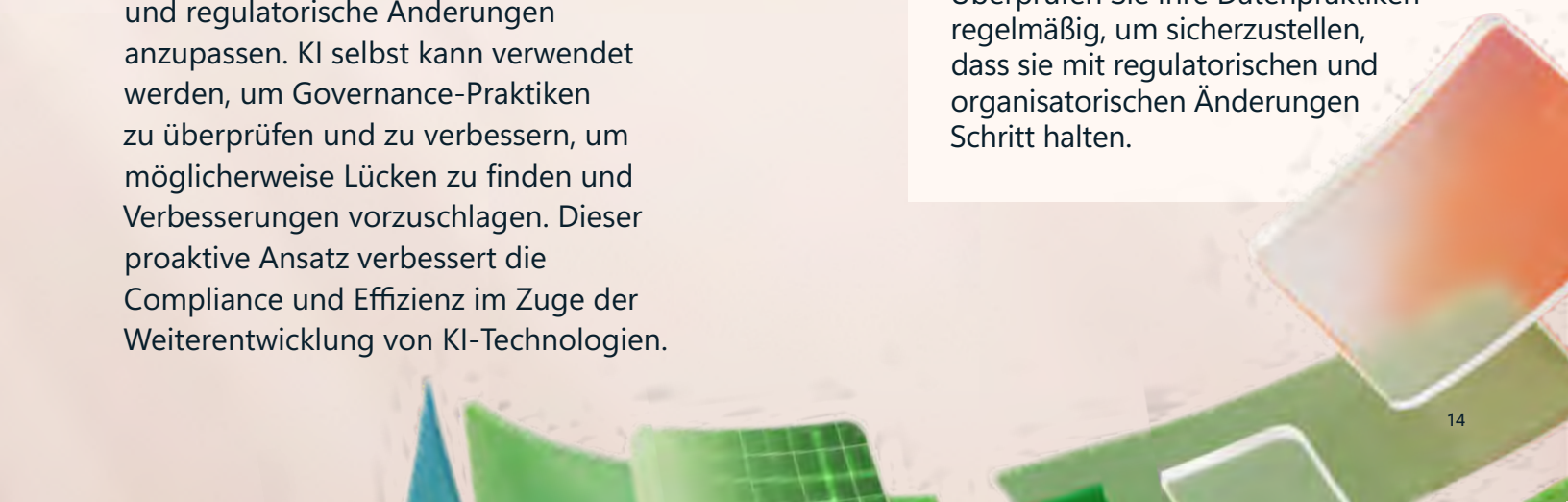
Ausrichtung an den Unternehmenszielen: Stellen Sie sicher, dass Ihre Data Governance-Strategie die Ziele Ihres Unternehmens unterstützt, um die Entscheidungsfindung und Effizienz zu verbessern.

Automatisieren von Routineaufgaben: Nutzen Sie Automatisierung für repetitive Aufgaben wie Datenklassifizierung und Zugriffsverwaltung, um manuelle Fehler zu reduzieren und die Sicherheit zu verbessern.

Sicherstellen von hohen Genauigkeitsstandards: Verwenden Sie Validierungs- und Bereinigungstools, um die Datenintegrität im Laufe der Zeit zu unterstützen.

Schulen von Benutzenden: Bieten Sie Schulungen zu Data Governance-Tools und -Verfahren an, um Missmanagement zu verhindern und die Einhaltung von Richtlinien sicherzustellen.

Durchführen von regelmäßigen Audits: Überprüfen Sie Ihre Datenpraktiken regelmäßig, um sicherzustellen, dass sie mit regulatorischen und organisatorischen Änderungen Schritt halten.



Fazit

Effektive Data Governance für KI-Unterstützung mit Microsoft 365

Ein verantwortungsvoller Umgang mit KI erfordert eine robuste Data Governance. Eine effektive Data Governance gewährleistet Datenverfügbarkeit, -genauigkeit und -sicherheit. Dadurch kann KI zuverlässige Insights liefern und Innovationen vorantreiben. Die Priorisierung von Datenqualität, Compliance und Sicherheit optimiert die KI-Funktionen. Dies sorgt wiederum dafür, dass die Entscheidungsfindung verbessert wird und der Wettbewerbsvorteil eines Unternehmens erhalten bleibt.

Microsoft 365: Unterstützung der KI-Readiness

Microsoft 365 bietet erstklassige Produktivitäts-Apps mit integrierten Tools für Datenklassifizierung, -kontrolle und -schutz. Diese Funktionen unterstützen Ihr Data Governance-Framework und ermöglichen eine sichere KI-Einführung, wenn Sie dazu bereit sind. Microsoft 365 hilft Ihnen, Folgendes sicherzustellen:

- **Datenqualität:** Unterstützung von Genauigkeit und Zuverlässigkeit für KI-Ausgaben
- **Compliance:** Einhaltung regulatorischer Anforderungen und Reduzierung rechtlicher Risiken
- **Zero-Trust-Sicherheit:** Schutz von vertraulichen Informationen vor nicht autorisiertem Zugriff, Sicherheitsverletzungen und Cyberbedrohungen

Entdecken Sie umfassende Produktivitätstools mit KI-Optionen und robustem Schutz, damit Ihr Unternehmen effizient und sicher arbeiten kann.

Microsoft 365 entdecken