Microsoft

DSGVO & Generative KI

Leitfaden für Geschäftskunden

Stand: Januar 2025

Inhalt

Executive Summary

- Aktuelle Anwendungsfälle für generative KI bieten ein enormes Potenzial, um die Qualität von Services und die operative Effizienz zu verbessern. Wir bei Microsoft möchten unsere Kunden in die Lage versetzen, das volle Potenzial neuer Technologien wie generativer künstlicher Intelligenz (generative KI, GenAI) zu nutzen und gleichzeitig ihren Verpflichtungen im Sinne der EU-Datenschutz-Grundverordnung (DSGVO) nachzukommen.
- Microsoft setzt sich dafür ein, dass seine KI-Systeme verantwortungsbewusst und auf eine Weise entwickelt werden, in die Menschen vertrauen können. Wir treiben dieses Engagement anhand von sechs Kernprinzipien voran, die eng an die in Artikel 5 der DSGVO dargelegten Grundsätze angelehnt sind.
- Bei der Prüfung der DSGVO-Compliance im Zusammenhang mit der Nutzung generativer KI-Dienste gelten die Grundsätze der DSGVO in gleicher Weise wie für die Verarbeitung personenbezogener Daten in jedem anderen Kontext (z. B. bei der Nutzung von Cloud-Diensten). Auch wenn KI-Technologien vergleichsweise jung sind, bleiben die Prinzipien und dementsprechend die Prozesse für die Risikobewertung und DSGVO-Compliance die gleichen. In Bezug auf die DSGVO können Unternehmen daher die KI-Services von Microsoft auf die gleiche Weise bewerten, wie sie es bei der Nutzung anderer Cloud-Dienste tun.
- Die bestehenden Datenschutzverpflichtungen von Microsoft, einschließlich der in unserem Data Protection Addendum enthaltenen Verpflichtungen, erstrecken sich auch auf unsere kommerziellen KI-Produkte. Kunden können sich darauf verlassen, dass die Datenschutzverpflichtungen, auf die sie sich bei der Nutzung unserer Enterprise-Cloud-Produkte seit langem verlassen, auch für Microsoft 365 Copilot und den Azure OpenAI Service gelten. Kunden können sicher sein, dass ihre wertvollen Daten durch branchenführende Data-Governance- und Datenschutzpraktiken in der vertrauenswürdigsten Cloud auf dem heutigen Markt geschützt werden.
- Es gibt eine Reihe von zentralen Verpflichtungen im Rahmen der DSGVO, die Unternehmen bei der Nutzung generativer KI-Dienste berücksichtigen müssen. Dieses Dokument beschreibt Details zu diesen Verpflichtungen und der damit verbundenen Unterstützung sowie hilfreichen Ressourcen, die Microsoft anbieten kann. Dazu zählen Informationen zu internationalen Übertragungen von personenbezogenen Daten, Transparenz, Betroffenenrechte, Pflichten von Auftragsdatenverarbeitern, technische und organisatorische Sicherheitsmaßnahmen und DSFAs.
- Die Daten unserer Kunden gehören unseren Kunden. Microsoft erhebt keinen Anspruch auf das Eigentum an Kunden-Prompts oder Output-Inhalten, die von den generativen KI-Lösungen von Microsoft erstellt werden. Ohne Zustimmung des Kunden werden auch keine Kundendaten (einschließlich Prompts oder Outputs) zum Trainieren von Foundation-Modellen verwendet.
- Da sich das regulatorische Umfeld beständig weiterentwickelt und Microsoft Innovationen vorantreibt, um neue Arten von KI-Lösungen bereitzustellen, werden wir weiterhin branchenführende Tools, Ressourcen und Support anbieten, um unser anhaltendes Engagement für die Erfüllung der Bedürfnisse und Anforderungen unserer Kunden auf ihrem Weg zur KI zu demonstrieren.

Einführung

Die enorme Dynamik des heutigen Wirtschaftsumfelds verlangt von Unternehmen in allen Branchen, innovativ und dabei effizienter zu sein und die Kundenerlebnisse zu verbessern. Um diese Ziele zu erreichen und ihren Wettbewerbsvorteil auszubauen, setzen Unternehmen vermehrt auf das Potenzial generativer KI-Lösungen. Diese können Routineaufgaben automatisieren, tiefgreifende analytische Insights liefern und die Entscheidungsfindung in Echtzeit unterstützen.

KI wird die Arbeitsweise von Unternehmen grundlegend verändern. Der geschäftliche Nutzen liegt auf der Hand: KI hilft Unternehmen, effizient zu arbeiten, bessere Leistungen zu erbringen, mehr zu erreichen und die erforderlichen Erkenntnisse zu gewinnen, mit denen sie bessere Entscheidungen treffen. Schon jetzt zeigt sich, dass sich Investitionen in KI-Lösungen positiv auf die Geschäftsergebnisse auswirken.[1]

GenAI-Lösungen können Ihre Organisation auf allen Ebenen optimieren und neue wertvolle Potenziale aufdecken. Um KI-Innovationen wirklich gewinnbringend zu nutzen, muss sichergestellt sein, dass Ihre Organisation sich für effiziente und vertrauenswürdige KI-Lösungen entscheidet und dass diese auf verantwortungsvolle und sichere Weise implementiert werden – insbesondere im Hinblick auf den Datenschutz.

Microsoft möchte seine Kundinnen und Kunden in die Lage versetzen, das volle Potenzial neuer Technologien wie generativer KI auszuschöpfen und gleichzeitig ihren Verpflichtungen im Zusammenhang mit der EU-Datenschutz-Grundverordnung (DSGVO) nachzukommen.

Unsere langjährige Erfahrung und unsere starken Maßnahmen für den Schutz von Kundendaten fließen unmittelbar in unseren Ansatz für verantwortungsvolle KI ein – mit klaren Grundprinzipien für Datenschutz, Sicherheit und Absicherung unserer GenAI-Produkte und -Lösungen. Unsere Kunden können sich darauf verlassen, dass ihre wertvollen Daten durch führende Data-Governance- und Datenschutzpraktiken in einer der vertrauenswürdigsten Clouds geschützt werden – und dass sie von den gleichen Datenschutzverpflichtungen wie bei unseren Enterprise-Cloud-Produkten profitieren. Entsprechend gilt für unsere generativen KI-Lösungen – einschließlich Microsoft 365 Copilot und Azure OpenAI Service – auch das Data Protection Addendum.

Als Branchenführer und Vordenker im Bereich KI haben wir diesen Leitfaden entwickelt, um spezifische Bedenken im Zusammenhang mit der DSGVO-konformen Nutzung von Microsoft 365 Copilot und Azure OpenAI Service für Kunden in Europa auszuräumen und um darzulegen, wie unsere KI-Lösungen DSGVO-konform genutzt werden können.

[1] Für jeden US-Dollar, den ein Unternehmen in KI investiert, erzielt es einen durchschnittlichen ROI von 3,50 US-Dollar, und es dauert durchschnittlich 14 Monate, bis Unternehmen eine Rendite auf ihre KI-Investition erzielen. Quelle: IDC, The Business Opportunity of AI, November 2023

Dieser Leitfaden ist wie folgt aufgebaut:

Teil 1

beschreibt die Bedeutung von verantwortungsvoller KI, die sechs Kernprinzipien und den Ansatz für verantwortungsvolle KI von Microsoft, der bei der Entwicklung von KI-Produkten zum Tragen kommt, und stellt Tools und Ressourcen für die Unterstützung Ihrer KI-Bereitstellung vor.

Teil 2

legt den Fokus auf die Struktur und die Anforderungen der DSGVO und beschreibt, wie Microsoft Kunden dabei unterstützen kann, unsere KI-Lösungen zu nutzen und gleichzeitig ihre Compliance-Verpflichtungen im Rahmen der DSGVO zu erfüllen.

Teile 3 und 4

widmen sich einer eingehenden Untersuchung von Microsoft 365 Copilot und dem Azure OpenAI Service und stellen dar, wie diese Dienste in Übereinstimmung mit der DSGVO genutzt werden können.

Teil 5

bildet den Abschluss des Leitfadens – mit einer Zusammenfassung der Insights sowie einem Ausblick auf die zukünftige Entwicklung der KI- und Datenschutzregulierung.

Anhang 1

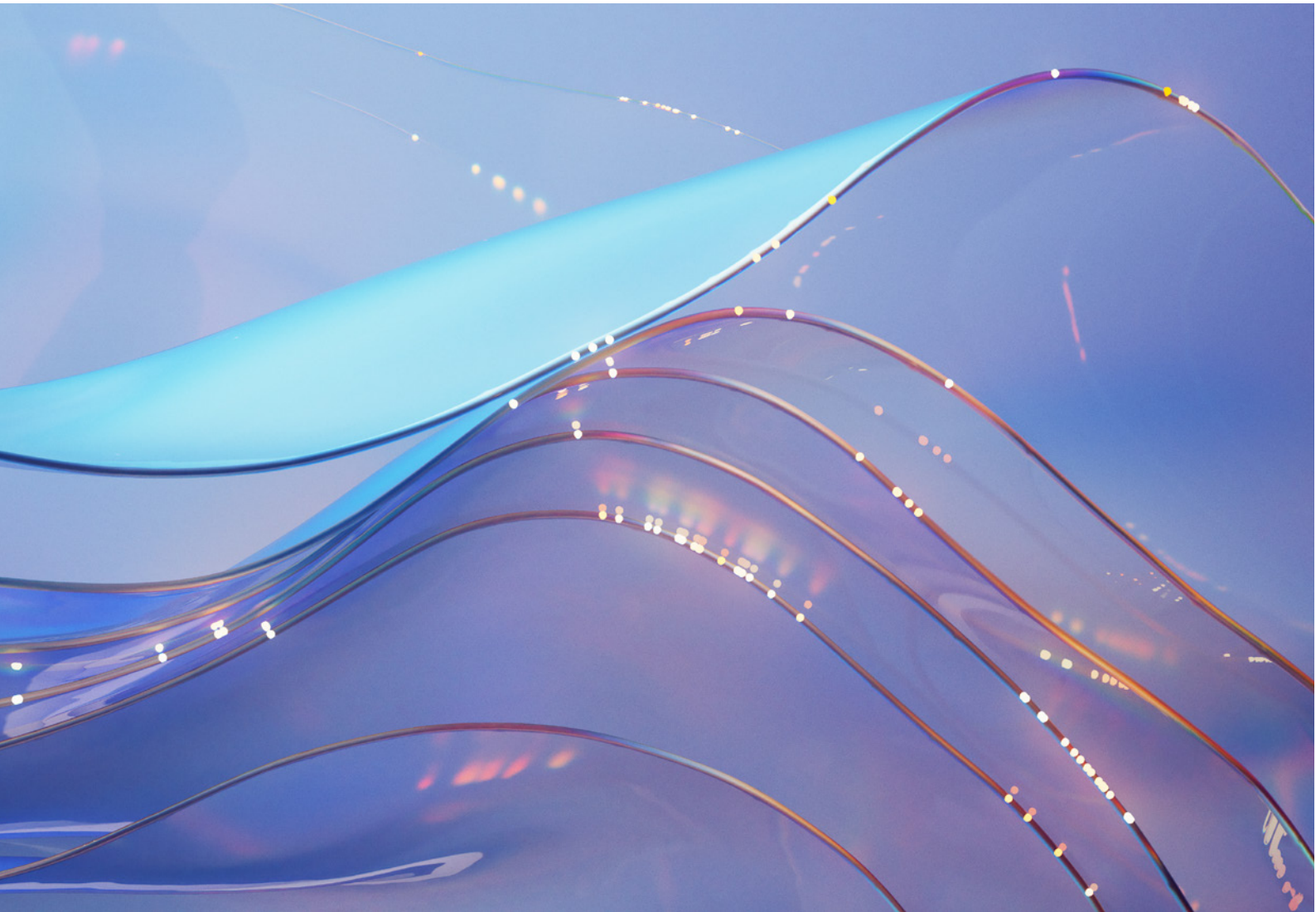
liefert Beispiele für die vielen interessanten Möglichkeiten, die generative KI für Unternehmen in verschiedenen Branchen bietet.

Anhang 2

beantwortet einige häufig gestellte Fragen (FAQs), die Kunden in Bezug auf den DSGVO-konformen Einsatz von KI haben.

Anhang 3

bietet Links zu weiterführenden Ressourcen, die Kunden nutzen können, um sich im Detail über weitere Aspekte zu den in diesem Leitfaden behandelten Themen zu informieren.



Teil 1

KI verantwortungsvoll einsetzen: Die Microsoft AI Journey und die Nutzung unserer Tools und Ressourcen

Verantwortungsvolle KI

KI hat das Potenzial, Ihr Unternehmen zu transformieren – von der Rationalisierung einzelner Aufgaben im Tagesgeschäft bis hin zur Beschleunigung Ihrer Service- und Lieferprozesse. Das wachsende Interesse an generativer KI ist offensichtlich. Jedoch geht mit dieser großen „Macht" auch eine große Verantwortung einher: KI muss verantwortungsvoll entwickelt und eingesetzt werden. Microsoft übernimmt in diesem Bereich mit der Entwicklung umfassender „Responsible AI"-Richtlinien und -Tools, die auf unserer langjährigen Arbeit basieren, eine führende Rolle.

Der verantwortungsvolle Umgang mit KI ist ein Thema, mit dem sich Unternehmen auf der ganzen Welt in den letzten Jahren aktiv auseinandergesetzt haben. Parallel zu intensiven theoretischen Diskussionen, der Entwicklung wegweisender Ansätze und Strategien sowie deren Umsetzung in die Praxis nimmt die KI-Nutzung weiter zu.

Mehr erfahren Sie im Whitepaper „Governing AI: A Blueprint for the Future".

Wir bei Microsoft setzen uns dafür ein, dass KI-Systeme verantwortungsvoll und auf eine Weise entwickelt werden, die das Vertrauen der Menschen verdient. Wir treiben dieses Engagement nach **sechs Prinzipien** voran, die eng an die in **Artikel 5 der DSGVO festgelegten Grundsätze** angelehnt sind:

- **Fairness:** KI-Systeme müssen so konzipiert sein, dass sie alle Menschen fair und ohne Vorurteile oder Diskriminierung behandeln.
- **Zuverlässigkeit und Sicherheit:** KI-Systeme müssen zuverlässig und sicher funktionieren und über integrierte Mechanismen verfügen, um Fehler zu vermeiden und Schäden zu minimieren.
- **Verantwortlichkeit:** Entwickler von KI-Tools und Entwickler, die sie nutzen, müssen für ihre Systeme verantwortlich sein.
- **Datenschutz und -sicherheit**: KI-Systeme müssen die Privatsphäre und Datensicherheit des Einzelnen achten und schützen.
- **Inklusion:** KI-Systeme müssen so konzipiert sein, dass sie für alle, auch für Menschen mit Behinderungen, zugänglich und nutzbar sind.
- **Transparenz:** KI-Systeme müssen verständlich sein, mit einer klaren Dokumentation ihrer Funktionsweise und Entscheidungsprozesse.

Anhand dieser Prinzipien können Kunden im Rahmen der DSGVO ihre KI-Systeme und -Prozesse evaluieren, die sie im Einsatz haben oder für die Zukunft in Betracht ziehen, wie in Teil 2 erläutert. Bei Microsoft wurde intern das Office of Responsible AI eingerichtet, das KI-Governance-Richtlinien für das gesamte Unternehmen festlegt, unser Führungsteam in KI-Fragen berät, die Entwicklungs- und Compliance-Teams in der gesamten Organisation unterstützt, Lösungen auf Grundlage der Responsible-AI-Prinzipien zu erstellen, und gleichzeitig sicherstellt, dass wir als Unternehmen unsere ethische Haltung kontinuierlich überprüfen und verbessern, während sich neue Funktionen und Herausforderungen entwickeln.

Erfahren Sie mehr über die Prinzipien und den Ansatz von Microsoft für verantwortungsvolle KI.

Im Mai 2024 haben wir unseren ersten Responsible AI Transparency Report veröffentlicht, der auf unserem internen Microsoft Responsible AI-Standard aufbaut. Dieser Bericht gibt Aufschluss darüber, wie wir Anwendungen entwickeln, die generative KI verwenden, wie wir Entscheidungen treffen und die Bereitstellung dieser Anwendungen überwachen, wie wir Kunden bei der Entwicklung ihrer eigenen generativen KI-Anwendungen unterstützen und wie wir bei Microsoft lernen, uns weiterentwickeln und als verantwortungsbewusste KI-Community wachsen.

Jedes Unternehmen sollte selbst verantwortungsvolle KI-Strategien – einschließlich Prinzipien, Praktiken, Tools und Governance – definieren und diese als Orientierung vorgeben, damit ihre Mitarbeitenden die eigene Nutzung von KI evaluieren, reflektieren und steuern können.

Wenn potenzielle Risiken verstanden und sorgfältig gesteuert werden, können Unternehmen das immense Potenzial von KI ausschöpfen. Vorausschauende Führungskräfte werden dafür Sorge tragen, dass ihr Engagement für verantwortungsvolle KI von Beginn an in der Innovationspipeline ihres Unternehmens verankert wird. So können sich Unternehmen die Leistungsfähigkeit von KI zunutze machen, um ihre Produkte und/oder Dienstleistungen zu verbessern und ihre Rentabilität zu steigern. Interessante Beispiele für den Einsatz von generativer KI finden Sie in Anhang 1.

Tools, Verpflichtungen und Ressourcen zur Unterstützung Ihrer KI-Bereitstellung

Um unsere Kunden zu unterstützen und sie bei ihrer KI-Compliance zu begleiten, bietet Microsoft eine Reihe von Lösungen, Tools und Ressourcen an – von umfassender Transparenz-Dokumentation bis hin zu einer Suite von Tools für Data-Governance-, Risiko- und Compliance-Bewertungen. Spezielle Programme wie unser branchenführendes AI Assurance-Programm und AI Customer Commitments dehnen diese Unterstützung für unsere Kunden aus, indem wir ihre Anforderungen erfüllen.

Unser AI Assurance-Programm hilft Kunden sicherzustellen, dass die KI-Anwendungen, die sie auf unseren Plattformen bereitstellen, die gesetzlichen und behördlichen Anforderungen für verantwortungsvolle KI erfüllen. Das Programm umfasst Unterstützung bei der regulatorischen Einbindung und eine Interessenvertretung, die Implementierung eines Risiko-Frameworks und die Einrichtung eines Customer Councils.

Seit Jahrzehnten verteidigen wir unsere Kunden gegen Ansprüche auf geistiges Eigentum in Bezug auf unsere Produkte.

Aufbauend auf unseren früheren AI Customer Commitments hat Microsoft ein Customer Copyright Commitment angekündigt, das unsere Unterstützung für Entschädigungen im Hinblick auf geistiges Eigentum sowohl auf Microsoft 365 Copilot als auch auf unseren Azure OpenAI Service ausweitet. Wenn nun ein Dritter einen Kunden wegen Urheberrechtsverletzung verklagt, weil er Microsoft 365 Copilot oder den Azure OpenAI Service oder für den von diesen Diensten generierten Output verwendet, verteidigen wir den Kunden und übernehmen die Strafzahlungen aus allen nachteiligen Urteilen oder Vergleichen, die aus der Klage resultieren, sofern der Kunde die Leitplanken und Content-Filter verwendet hat, die wir in unsere Produkte integriert haben.

Microsoft hat zudem unter der Produktbezeichnung „Microsoft Purview" mehrere Lösungen entwickelt, um Sie als Kunden bei der Data Governance zu unterstützen. Wie Microsoft Purview Sie bei der DSGVO-Compliance unterstützen kann, erfahren Sie in Teil 2.

Teil 2

Das DSGVO-Compliance-Framework im Kontext von KI

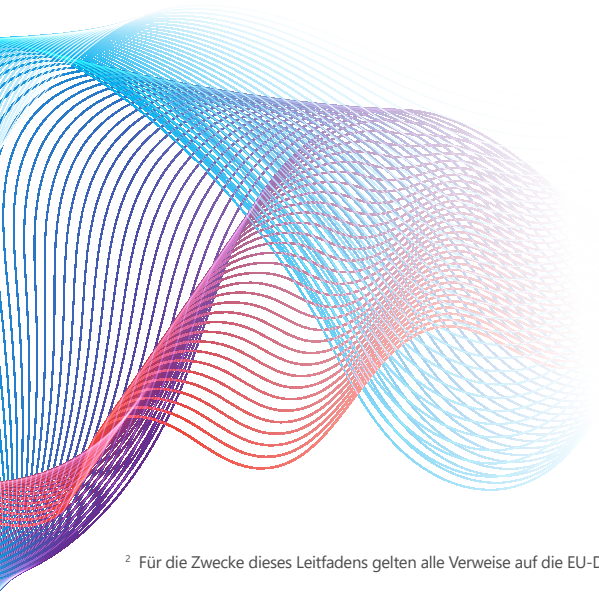
Was ist die DSGVO und für wen gilt sie?

Die EU-Datenschutz-Grundverordnung, auch als „DSGVO"[2] bezeichnet, setzt weltweit einen wichtigen Standard für Datenschutzrechte, Informationssicherheit und Compliance. Wir bei Microsoft schätzen den Datenschutz als Grundrecht und sind überzeugt, dass die DSGVO eine wichtige Rolle beim Schutz und der Förderung der Datenschutzrechte des Einzelnen spielt.

Microsoft verpflichtet sich zur Einhaltung der DSGVO und stellt eine Reihe von Produkten, Funktionen, Dokumentationen und Ressourcen bereit, um unsere Kunden bei der Erfüllung ihrer Compliance-Verpflichtungen im Rahmen der DSGVO zu unterstützen.

Die DSGVO ist in Großbritannien und in allen EU-Ländern in Kraft und schreibt eine Reihe von Datenschutzvorschriften für die Verarbeitung personenbezogener Daten vor, mit dem Ziel, die Grundrechte betroffener Personen zu schützen, gleiche Wettbewerbsbedingungen für die Verarbeitung personenbezogener Daten zu schaffen und den Binnenmarkt zu fördern.

Jede Organisation, die personenbezogene Daten von betroffenen Personen mit Wohnsitz in Europa verarbeitet, unterliegt der DSGVO. In den nationalen Gesetzen sind auch Datenschutzvorschriften und -richtlinien enthalten. Diese sind in der Regel weiter verfeinert worden, um die Anforderungen der DSGVO zu erfüllen und/oder zu übertreffen.



Nutzung etablierter Prinzipien zur Einhaltung gesetzlicher Rahmenbedingungen beim Einsatz von KI-Lösungen

Wenn wir die DSGVO im Zusammenhang mit der Nutzung generativer KI und der Nutzung der Möglichkeiten dieser Technologie betrachten, ist der Ausgangspunkt, dass die Grundprinzipien der DSGVO immer noch in der gleichen Weise gelten wie für die Verarbeitung personenbezogener Daten in jedem anderen Kontext, auch bei der Nutzung der Cloud.

Auch wenn die KI-Technologie vergleichsweise jung ist, bleiben die Prinzipien und dementsprechend die Prozesse für die Risikobewertung und die Einhaltung der DSGVO die gleichen.

Es ist auch hilfreich zu wissen, dass die DSGVO technologieunabhängig formuliert wurde und für Unternehmen daher keinen Hinderungsgrund darstellt, Möglichkeiten zum Einsatz generativer KI zu nutzen.

Die Anwendung etablierter DSGVO-Bewertungsprozesse ist somit für Unternehmen auch die Chance, das revolutionäre Potenzial von KI zu nutzen und bessere Ergebnisse zu erzielen, während gleichzeitig Datenschutz- und Persönenrechte geschützt bleiben. Microsoft arbeitet seit jeher eng mit seinen Kunden zusammen: Wir unterstützen sie bei der Verfolgung ihrer Prioritäten für die digitale Transformation und erfüllen gleichzeitig die Anforderungen der DSGVO, auch in Bezug auf den Übergang von On-Premises-Systemen zu Cloud Computing. Kunden können sich den generativen KI-Lösungen von Microsoft nähern, indem sie einen ähnlichen Ansatz wie bei der Entscheidung für unsere Clouddienste verfolgen.

Cloud Computing ist für den Zugang zu potenziell bahnbrechender KI-Technologie unerlässlich, und die Hyperscale-Cloud bildet somit auch die Grundlage für den Einsatz von KI. Die hochgradigen Schutzmaßnahmen von Azure, die Teil von Microsoft 365 Copilot und dem Azure OpenAI Service sind, bieten eine solide Grundlage, auf der Kunden ihre eigenen Datenschutz-, Sicherheits- und Compliance-Systeme aufbauen können, um KI sicher zu skalieren und gleichzeitig Risiken zu steuern und die Einhaltung der DSGVO sicherzustellen.

[2] Für die Zwecke dieses Leitfadens gelten alle Verweise auf die EU-DSGVO auch für die UK GDPR.

Wer ist für die Einhaltung der DSGVO bei der Nutzung von KI und Cloud-Diensten verantwortlich?

Im Rahmen der DSGVO gibt es zwei Hauptparteien mit jeweils unterschiedlichen Compliance-Verantwortlichkeiten:

- **Der Datenverantwortliche:** Der für die Datenverarbeitung Verantwortliche entscheidet, warum und wie personenbezogene Daten verarbeitet werden, und ist die Organisation, die das Hauptsubjekt der durch die DSGVO auferlegten Verpflichtungen ist. Viele dieser Verpflichtungen gelten ab dem Zeitpunkt, an dem diese Organisation beginnt, personenbezogene Daten zu Einzelpersonen zu erfassen.
- **Der Datenverarbeiter:** Im Gegensatz dazu ist der Datenverarbeiter nach der DSGVO im Wesentlichen ein Subunternehmer des für die Verarbeitung Verantwortlichen, der personenbezogene Daten im Auftrag und auf Anweisung des für die Verarbeitung Verantwortlichen verarbeitet.

Organisationen können im Rahmen der DSGVO als Datenverantwortliche und Datenverarbeiter fungieren. Bei der Nutzung der generativen KI-Dienste von Microsoft geben die Produktbedingungen von Microsoft an, ob Microsoft einen Onlinedienst als Datenverarbeiter oder Datenverantwortlicher bereitstellt. Die meisten Onlinedienste, einschließlich generativer KI-Dienste, werden von Microsoft als Datenverarbeiter bereitgestellt und unterliegen dem Data Protection Addendum. Weitere Informationen zu den einzelnen Produkten und Diensten finden Sie in den Microsoft Privacy & Security Terms.

Die Einhaltung der DSGVO ist eine gemeinsame Verantwortung

Die Einhaltung der DSGVO ist eine gemeinsame Verantwortung. Microsoft verpflichtet sich, alle Gesetze und Vorschriften einzuhalten, die für Microsoft und seine generativen KI-Tools und -Dienste gelten, einschließlich der DSGVO.

Als Microsoft-Kunde müssen Sie festlegen, wie diese Tools und Dienste verwendet werden und welche personenbezogenen Daten verarbeitet werden, damit Sie sicherstellen können, dass Sie diese Tools auf Compliance-gerechte Weise verwenden.

Um Sie dabei zu unterstützen, haben wir unsere generativen KI-Tools und -Dienste unter Berücksichtigung der Privatsphäre und des Datenschutzes entwickelt und stellen unseren Kunden Informationen, Funktionen und vertragliche Verpflichtungen zur Verfügung, um Sie bei Ihren Compliance- und Rechenschaftspflichten gemäß der DSGVO zu unterstützen. In den folgenden Abschnitten in Teil 2 wird näher auf diese Themen eingegangen. Dort finden Sie Informationen, die Sie bei der Bewertung der Nutzung der generativen KI-Tools und -Dienste von Microsoft in Übereinstimmung mit der DSGVO unterstützen sollen.

Wie unterstützt Microsoft Kunden bei der Einhaltung der DSGVO?

Da immer mehr Unternehmen auf generative KI setzen, sehen viele Microsoft nicht nur als Service Provider, sondern auch als vertrauenswürdigen Partner auf dem Weg, ihnen bei der Erfüllung ihrer Compliance-Verpflichtungen im Rahmen der DSGVO zu helfen.

Der erste Schritt zur Compliance besteht darin, zu verstehen, wie die generativen KI-Dienste von Microsoft funktionieren, einschließlich der Art und Weise, wie sie personenbezogene Daten verarbeiten. Unsere umfassende Transparenzdokumentation und -informationen helfen Ihnen zu verstehen, wie unsere KI-Tools funktionieren und welche Entscheidungen unsere Kunden treffen können, um die Systemleistung und das Systemverhalten zu beeinflussen.

In Teil 3 und Teil 4 dieses Dokuments stellen wir spezifische Informationen und Links zu zusätzlichen Ressourcen bereit, die Sie nutzen können, um Ihr Verständnis für diese Produkte und Dienste zu verbessern.

In Teil 3 erfahren Sie mehr über Microsoft 365 Copilot.

In Teil 4 erfahren Sie mehr über Azure OpenAI Service.

Dieses Wissen bildet die Grundlage für die Einhaltung einer Reihe wichtiger Verpflichtungen aus der DSGVO. Wir werden diese wichtigen Verpflichtungen und die damit verbundene Unterstützung, die Microsoft seinen Kunden bietet, weiter unten in diesem Abschnitt untersuchen, aber zuerst befassen wir uns mit den sieben wichtigsten Datenschutzverpflichtungen, die Microsoft seinen Kunden im KI-Zeitalter anbietet.

Schutz der Daten unserer Kunden – Microsoft und seine Datenschutzverpflichtungen im KI-Zeitalter

Die bestehenden Datenschutzverpflichtungen von Microsoft erstrecken sich auch auf unsere kommerziellen KI-Produkte, wie in einem Blogbeitrag von unserem Chief Privacy Officer Julie Brill erläutert. Sie können sicher sein, dass die Datenschutzverpflichtungen, auf die Sie sich bei der Nutzung unserer Enterprise-Cloud-Produkte seit langem verlassen, auch für unsere generativen KI-Lösungen für Unternehmen gelten, die durch das Microsoft Data Protection Addendum abgedeckt werden, einschließlich Microsoft 365 Copilot und Azure OpenAI Service.

Die folgenden sieben Verpflichtungen gelten für „Kundendaten", die in den Microsoft Product Terms als alle Daten definiert sind, einschließlich aller Text-, Ton-, Video- oder Bilddateien und Software, die Microsoft von oder im Namen unserer Kunden durch die Nutzung eines Onlinedienstes zur Verfügung gestellt werden. Alle Eingaben (einschließlich Prompts)[3] und Output-Inhalte[4] sind ebenfalls Kundendaten. In Übereinstimmung mit dem Microsoft Data Protection Addendum behält der Kunde „alle Rechte, Titel und Interessen an Kundendaten".

1. **Wir halten die Daten Ihres Unternehmens privat.**

   Ihre Daten bleiben bei der Nutzung von Microsoft 365 Copilot und Azure OpenAI Service privat und unterliegen unseren geltenden Datenschutz- und Vertragsverpflichtungen, einschließlich der Verpflichtungen, die wir im Microsoft Data Protection Addendum und den Microsoft Product Terms eingehen.

2. **Sie haben die Kontrolle über die Daten Ihrer Organisation.**

   Ihre Daten werden nicht auf geheime Weise oder ohne Ihre Zustimmung verwendet. Sie können Ihre Nutzung von Microsoft 365 Copilot oder Azure OpenAI Service anpassen und Ihre Daten zur Feinabstimmung von Modellen für die eigene Verwendung in Ihrer Organisation verwenden. Wenn Sie die Daten Ihrer Organisation für die Feinabstimmung verwenden, stehen alle fein abgestimmten KI-Lösungen, die mit den Daten Ihrer Organisation erstellt wurden, nur Ihnen zur Verfügung.

3. **Ihre Zugriffskontrolle und Unternehmensrichtlinien werden beibehalten.**

   Um den Datenschutz in Ihrer Organisation zu unterstützen, wenn Sie Enterprise-Produkte mit generativen KI-Funktionen verwenden, gelten Ihre vorhandenen Berechtigungen und Zugriffssteuerungen weiterhin, um sicherzustellen, dass die Daten Ihrer Organisation nur den Benutzenden angezeigt werden, denen Sie die entsprechenden Berechtigungen erteilt haben.

4. **Die Daten Ihrer Organisation werden nicht freigegeben.**

   Microsoft gibt Ihre Daten nicht ohne Ihre Zustimmung an Dritte weiter. Ihre Daten, einschließlich der Daten, die durch die Nutzung von Microsoft 365 Copilot oder Azure OpenAI Service in Ihrer Organisation generiert werden – z. B. Prompts und Antworten – werden vertraulich behandelt und nicht an Dritte weitergegeben.

5. **Der Datenschutz und die Sicherheit Ihrer Organisation sind „by Design" geschützt.**

   Sicherheit und Datenschutz werden in allen Phasen des Designs und der Implementierung von Microsoft 365 Copilot und Azure OpenAI Service berücksichtigt. Wie bei allen unseren Produkten bieten wir eine starke Datenschutz- und Sicherheitsbasis und stellen zusätzliche Schutzmaßnahmen zur Verfügung, die Sie aktivieren können. Da sich externe Bedrohungen weiterentwickeln, werden wir unsere Lösungen und Angebote weiter verbessern, um erstklassigen Datenschutz und Sicherheit in Microsoft 365 Copilot und Azure OpenAI Service zu gewährleisten, und wir werden unseren Ansatz weiterhin transparent gestalten.

6. **Die Daten Ihrer Organisation werden nicht zum Trainieren von Foundation-Modellen verwendet.**

   Die generativen KI-Lösungen von Microsoft, einschließlich Microsoft 365 Copilot und Azure OpenAI Service-Funktionen, verwenden ohne Ihre Erlaubnis keine Kundendaten zum Trainieren von Foundation-Modellen. Ihre Daten stehen OpenAI niemals zur Verfügung oder werden zur Verbesserung von OpenAI-Modellen verwendet.

[3] „Eingaben" (Inputs) bezeichnen alle Kundendaten, die der Kunde zur Verwendung durch eine generative Technologie der künstlichen Intelligenz bereitstellt, bezeichnet, auswählt oder eingibt, um eine Ausgabe (Output) zu generieren oder anzupassen, einschließlich aller Kunden-Prompts.

[4] „Output-Inhalt" (Content) bezeichnet alle Daten, Texte, Sounds, Videos, Bilder, Code oder andere Inhalte, die von einem Modell als Reaktion auf Eingaben generiert werden.

7. Unsere Produkte und Lösungen entsprechen den weltweiten Datenschutzbestimmungen.

Die von Ihnen bereitgestellten Microsoft AI-Produkte und -Lösungen entsprechen den heutigen globalen Datenschutzbestimmungen. Während wir weiterhin gemeinsam durch die Zukunft der KI navigieren, einschließlich der Umsetzung des EU AI Acts und anderer globaler Gesetze, können Organisationen sicher sein, dass Microsoft unsere Datenschutz- und Sicherheitspraktiken transparent macht. Wir werden die globalen Gesetze einhalten, die KI regeln, und unsere Versprechen mit klaren vertraglichen Verpflichtungen untermauern.

Weitere Informationen darüber, wie die Datenschutzverpflichtungen von Microsoft für Azure OpenAI und Microsoft 365 Copilot gelten, finden Sie in diesem Blogbeitrag und in den FAQ: Schutz der Daten unserer Kunden aus Wirtschaft und öffentlichem Sektor im KI-Zeitalter.

Zentrale Pflichten der DSGVO im Zusammenhang mit generativen KI-Diensten

Es gibt eine Reihe von Verpflichtungen im Rahmen der DSGVO, die Unternehmen bei der Beschaffung von generativen KI-Diensten berücksichtigen müssen. In diesem Abschnitt werden einige der wichtigsten Verpflichtungen sowie der zugehörige Support und die Ressourcen behandelt, die Microsoft Ihrer Organisation anbieten kann, um Sie bei der Einhaltung zu unterstützen.

Artikel 12 bis 14 DSGVO Transparenz

Nach den Artikeln 12 bis 14 der DSGVO sind die für die Verarbeitung Verantwortlichen verpflichtet, betroffenen Personen bestimmte wichtige Informationen darüber zur Verfügung zu stellen, wie ihre personenbezogenen Daten verwendet werden. Diese Informationen müssen in prägnanter, transparenter, verständlicher und leicht zugänglicher Form in klarer und einfacher Sprache bereitgestellt werden. Diese Informationen werden häufig in Form einer Datenschutzerklärung zur Verfügung gestellt. Wenn Sie eine neue Technologie (z. B. Microsoft 365 Copilot oder Azure OpenAI Service) bereitstellen und beabsichtigen, diese Technologie auf eine Weise zu verwenden, die sich nicht in Ihren vorhandenen Datenschutzhinweisen widerspiegelt, müssen Sie Ihre Datenschutzhinweise entsprechend aktualisieren.

Wie wir Ihre Compliance unterstützen: Die Informationen, die in diesem Dokument dargelegt werden und in unseren unten aufgeführten Transparenzressourcen verfügbar sind, sollen Ihnen helfen zu verstehen, wie Microsoft 365 Copilot und Azure OpenAI Service Daten verarbeiten und in welchem Umfang zusätzliche Informationen (falls vorhanden) an betroffene Personen weitergegeben werden müssen. Weitere produktspezifische Informationen finden Sie unter:

Daten, Datenschutz und Sicherheit für Azure OpenAI Service

Daten, Datenschutz und Sicherheit für Microsoft 365 Copilot

Copilot for Dynamics 365 und Power Platform

Artikel 15 bis 21 DSGVO Auskunftsrecht der betroffenen Person

Gemäß der DSGVO müssen die für die Verarbeitung Verantwortlichen sicherstellen, dass sie in der Lage sind, ihrer Verpflichtung nachzukommen, auf Anfragen der betroffenen Personen im Zusammenhang mit der Ausübung ihrer Rechte nach den Artikeln 15 bis 21 der DSGVO zu antworten, erforderlichenfalls mit angemessener Unterstützung durch die Datenverarbeiter.

Wie wir Ihre Compliance unterstützen: Im Abschnitt „Data Subjects Rights; Assistance with Requests" des Microsoft Data Protection Addendum verpflichtet sich Microsoft dazu, Kunden (in einer Weise, die mit der Funktionalität der Dienste und der Rolle von Microsoft als Datenverarbeiter vereinbar ist) die Möglichkeit zu geben, Anfragen von betroffenen Personen zu erfüllen, die ihre Rechte gemäß der DSGVO ausüben.

Wenn Microsoft in Situationen, in denen personenbezogene Daten im Namen Ihrer Organisation verarbeitet werden, eine solche Anfrage direkt von einer betroffenen Person erhält, leitet Microsoft die betroffene Person weiter, damit diese ihre Anfrage stattdessen an Ihre Organisation richtet. Sie sind für die Beantwortung solcher Anfragen verantwortlich, aber Microsoft wird diesbezüglichen Anfragen in angemessener Weise zur Unterstützung nachkommen.

Microsoft hat zusätzliche Lösungen entwickelt, um seine Kunden bei der Beantwortung von Anfragen zu Rechten betroffener Personen zu unterstützen, z. B. Microsoft Purview und Purview eDiscovery. Die Funktionen dieser Produkte ermöglichen es unseren Kunden, ihre KI-Nutzung proaktiv zu steuern und sich an die sich entwickelnden gesetzlichen Anforderungen zu halten. Dies kann beispielsweise wertvoll sein, um die Effizienz bei der Beantwortung und Bearbeitung von Anfragen in Bezug auf das „Recht auf Zugang zu personenbezogenen Daten" und das „Recht auf Vergessenwerden" gemäß den Artikeln 15 und 17 der DSGVO zu verbessern.

Erfahren Sie mehr über Microsoft Purview und seine Funktionen, die Ihnen bei der Bereitstellung der generativen KI-Lösungen von Microsoft helfen können.

Artikel 28 DSGVO
Pflichten des Auftragsverarbeiters

Die DSGVO schreibt vor, dass eine Organisation, die als Datenverantwortlicher fungiert, nur dann Datenverarbeiter einsetzt, um personenbezogene Daten in ihrem Namen zu verarbeiten, wenn diese ausreichende Garantien bieten, um die wichtigsten Anforderungen der DSGVO zu erfüllen. Diese Schlüsselanforderungen sind in Artikel 28 der DSGVO beschrieben und beinhalten, dass sich die Datenverarbeiter zu Folgendem verpflichten:

- Unterauftragsverarbeiter nur mit Zustimmung des für die Verarbeitung Verantwortlichen einsetzen und für Unterauftragsverarbeiter haftbar bleiben
- Personenbezogene Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, auch in Bezug auf Übermittlungen
- Sicherstellen, dass Personen, die personenbezogene Daten verarbeiten, zur Vertraulichkeit verpflichtet sind
- Geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau für personenbezogene Daten zu gewährleisten
- Den für die Verarbeitung Verantwortlichen bei seinen Verpflichtungen unterstützen, auf Anfragen der betroffenen Personen im Sinne der DSGVO zu reagieren
- Anforderungen der DSGVO zur Benachrichtigung und Unterstützung bei Verstößen erfüllen
- Den für die Verarbeitung Verantwortlichen bei Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden unterstützen

- Personenbezogene Daten am Ende der Erbringung von Dienstleistungen löschen oder zurückgeben
- Den für die Verarbeitung Verantwortlichen beim Nachweis der Einhaltung der DSGVO unterstützen

Wie wir Ihre Compliance unterstützen:
Microsoft stellt seinen Kunden im Data Protection Addendum (DPA) die vertraglichen Verpflichtungen zur Verfügung, die für Datenverarbeiter gemäß Artikel 28 DSGVO vorgegeben sind. Sie finden diese spezifischen Verpflichtungen im Anhang zum DPA sowie im Hauptteil des DPA, in dem die substanziellen Anforderungen der DSGVO, einschließlich Artikel 28, ausführlich behandelt werden.

In diesem Zusammenhang ist es wichtig zu betonen, dass die DSGVO von den für die Verarbeitung Verantwortlichen nicht verlangt, ihre eigenen Datenschutzbedingungen für ihre Datenverarbeiter zu erstellen und zu verwenden. Der Europäische Datenschutzausschuss (EDSA) selbst erkennt an, dass es konform ist, die Standardbedingungen eines Cloud-Anbieters zu verwenden, sofern dieser die DSGVO und Artikel 28 einhält.[5]

Ein Hyperscale-Cloud-Anbieter bedient alle seine Kunden einheitlich. Die Vertragsstruktur muss genau widerspiegeln, wie die Dienste des Auftragsverarbeiters funktionieren und personenbezogene Daten schützen. Einheitlichkeit ist Standard bei Cloud-Diensten und macht Cloud-Dienste besser verwaltbar, skalierbar, sicherer und kostengünstiger als On-Premises-Lösungen. In einem mehrinstanzenfähigen Dienst kann sich eine von einem Kunden auferlegte Änderung auf alle Kunden auswirken, die den Dienst verwenden. Problematisch kann dies sein, wenn Kunden widersprüchliche oder sich gegenseitig ausschließende Anforderungen haben. Darüber hinaus kann die Einführung unterschiedlicher Sicherheitsmaßnahmen oder -standards für verschiedene Kunden die Sicherheit der Microsoft-Dienste als Ganzes untergraben. Daher ist es für Microsoft nicht möglich, seine operativen Prozesse zu ändern oder maßgeschneiderte vertragliche Verpflichtungen und/oder Vertragsstrukturen für einzelne Kunden zu erstellen.

Vor diesem Hintergrund müssen Kunden verstehen, dass die Erstellung eigener Datenverarbeitungsbedingungen bei der Zusammenarbeit mit Hyperscale-Cloud-Anbietern sie daran hindern kann, die reichhaltige Innovation von cloudbasierten generativen KI-Diensten zu nutzen.

[5] Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der DSGVO.

Artikel 32 DSGVO Sicherheitsmaßnahmen

Artikel 32 der DSGVO verpflichtet die für die Verarbeitung Verantwortlichen und die Datenverarbeiter, geeignete technische und organisatorische Maßnahmen zu ergreifen, um unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Mit diesen Maßnahmen sollten die Risiken im Zusammenhang mit der versehentlichen oder unrechtmäßigen Zerstörung, dem Verlust, der Veränderung, der unbefugten Offenlegung oder dem unbefugten Zugriff auf übermittelte, gespeicherte oder auf sonstige Weise verarbeitete personenbezogene Daten berücksichtigt werden.

Wie wir Ihre Compliance unterstützen:
In der Rubrik „Data Security" des Microsoft Data Protection Addendum verpflichtet sich Microsoft vertraglich, geeignete technische und organisatorische Maßnahmen zu implementieren und aufrechtzuerhalten, um „Kundendaten" und „personenbezogene Daten" vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung, unbefugter Offenlegung oder unbefugtem Zugriff auf solche übertragenen, gespeicherten oder anderweitig verarbeiteten Daten zu schützen.

Diese technischen Maßnahmen sind in der Sicherheitsrichtlinie von Microsoft umgesetzt und entsprechen ISO 27001, ISO 27002 und ISO 27018. Microsoft verpflichtet sich außerdem vertraglich zur Verschlüsselung von „Kundendaten" (einschließlich aller darin enthaltenen „personenbezogenen Daten"), und zwar während der Übertragung (einschließlich zwischen Microsoft-Rechenzentren) und im Ruhezustand. Im Anhang A „Security Measures" des DPA finden Sie umfassende Verpflichtungen von Microsoft in Bezug auf die Sicherheit von Kundendaten, einschließlich in Bezug auf die Organisation der Informationssicherheit, Asset Management, Human Resources Security, physische und Umweltsicherheit, Kommunikation und Operations Management, Informationssicherheit, Incident Management und Business Continuity Management.

Die oben beschriebenen technischen, organisatorischen und sicherheitsbezogenen Maßnahmen gelten für alle Kundendaten, die Kunden bei der Verwendung von Microsoft 365 Copilot und Azure OpenAI Service bereitstellen oder erstellen. Sie können sich auf die oben aufgeführten Informationen beziehen, um das Engagement und die Maßnahmen von Microsoft zum Schutz von Kundendaten (einschließlich personenbezogener Daten) zu demonstrieren.

In Teil 3 erfahren Sie mehr über die Sicherheit von Microsoft 365 Copilot.

In Teil 4 erfahren Sie mehr über die Sicherheit für Azure Open AI Service.

Artikel 35 DSGVO
Datenschutz-Folgenabschätzung

Nach Artikel 35 der DSGVO sind die für die Verarbeitung Verantwortlichen verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, wenn die Verarbeitung personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt (insbesondere, wenn dies den Einsatz neuer Technologien beinhaltet).

Bei der Beurteilung, ob eine DSFA erforderlich ist, müssen die für die Verarbeitung Verantwortlichen Art, Umfang, Inhalt und Zwecke der Verarbeitung berücksichtigen. Ob eine DSFA für die Nutzung von Microsoft 365 Copilot und Azure OpenAI Service erforderlich ist, hängt daher vom jeweiligen Anwendungsfall und der Art der personenbezogenen Daten ab, die Sie mit diesen Diensten verarbeiten möchten.

Erfahren Sie mehr darüber, wann eine DSFA abgeschlossen sein muss.

Auch wenn sie nicht gesetzlich vorgeschrieben ist, ist eine DSFA eine bewährte Methode und kann Ihnen helfen, die spezifischen Datenschutzrisiken zu bewältigen, die mit der Implementierung von Microsoft 365 Copilot und/oder Azure OpenAI Service für einen bestimmten Anwendungsfall verbunden sind. Die Erstellung einer DSFA kann Ihnen auch dabei helfen, Ihren Rechenschaftspflichten gemäß Artikel 5 Absatz 2 der DSGVO nachzukommen.

Eine DSFA muss mindestens Folgendes enthalten:

(a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

(b) eine Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf die Zwecke,

(c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

(d) die Maßnahmen, die zur Bewältigung der Risiken vorgesehen sind, einschließlich Garantien, Sicherheitsmaßnahmen und Mechanismen zur Gewährleistung des Schutzes personenbezogener Daten und zum Nachweis der Einhaltung der DSGVO unter Berücksichtigung der Rechte und berechtigten Interessen der betroffenen Personen und anderer betroffener Personen.

Erfahren Sie mehr über den Inhalt einer DSFA.

Wie wir Ihre Compliance unterstützen:
Die in diesem Dokument enthaltenen Informationen und die zusätzlichen Ressourcen, auf die es verweist, können Ihnen bei der Erstellung einer DSFA helfen, insbesondere:

- Die Informationen in Teil 3 und Teil 4, die sich darauf beziehen, wie Microsoft 365 Copilot und Azure OpenAI Service Daten verarbeiten, helfen bei der Vervollständigung der in (a) oben beschriebenen Elemente.
- Die Abschnitte zu technischen und organisatorischen Maßnahmen sowohl für Microsoft 365 Copilot als auch für Azure OpenAI Service helfen bei der Vervollständigung der oben unter (d) beschriebenen Elemente.

Die unter (b) und (c) beschriebenen Bewertungen variieren von Fall zu Fall je nach Anwendungsfall und Art, Umfang und Inhalt der betroffenen personenbezogenen Daten und müssen von Ihnen durchgeführt werden.

Erfahren Sie mehr über Datenschutz-Folgenabschätzungen für die DSGVO.

Artikel 44 bis 50 DSGVO
Übermittlung personenbezogener Daten an Drittländer

Die DSGVO erlaubt die Übermittlung personenbezogener Daten in ein Drittland außerhalb der EU oder des EWR (einschließlich der USA), wenn bestimmte Voraussetzungen erfüllt sind. Zu diesen Bedingungen gehört, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt oder wenn geeignete zusätzliche Garantien (wie die EU-Standardvertragsklauseln) eingeführt wurden.[6]

Wie wir Ihre Compliance unterstützen:
Alle Übertragungen personenbezogener Daten durch Microsoft außerhalb von UK, der EU oder des EWR unterliegen einem gültigen Übermittlungsmechanismus gemäß der DSGVO, einschließlich Übertragungen in die USA.

Die EU-Kommission und der britische Außenminister haben Angemessenheitsbeschlüsse bekannt gegeben, in denen sie feststellen, dass die USA (für die Zwecke von Artikel 45 der DSGVO) ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die aus UK oder der EU an Organisationen in den USA übermittelt werden, die nach dem EU-U.S. Data Privacy Framework zertifiziert sind. Microsoft ist nach diesem Framework und den damit verbundenen Verpflichtungen zertifiziert. Microsoft hat sich verpflichtet, das Framework zu unterstützen, und wird darüber hinausgehen, indem es alle Anforderungen erfüllt oder übertrifft, die dieses Framework für unsere Kunden umreißt.

Microsoft verwendet global auch weiterhin die EU-Standardvertragsklauseln und das UK Addendum, wo dies für Übertragungen aus UK, der EU oder Weiterleitungen angemessen ist – zum Vorteil unserer Kunden und ihrer Rechtssicherheit bei Übertragungen, die aus der EU stammen.

Zusätzlich zu den konformen Datenübertragungsmechanismen von Microsoft hat Microsoft die EU-Datengrenze definiert, die strenge Verpflichtungen für die Speicherung und Verarbeitung von Kundendaten innerhalb der EU vorsieht (siehe auch DPA und Product Terms), sodass die Übermittlung personenbezogener Daten in Drittländer reduziert und damit die Compliance mit der DSGVO bei Übermittlungen in Drittländer vereinfach wird. Sowohl Microsoft 365 Copilot als auch Azure OpenAI Services sind EU Data Boundary Services.

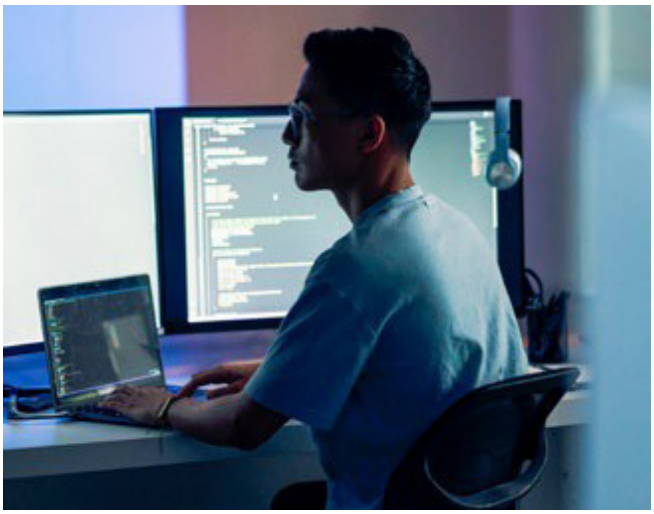
Die EU-Datengrenze ist eine geografisch definierte Grenze (bestehend aus den Ländern der EU und der Europäischen Freihandelsassoziation), innerhalb derer sich Microsoft verpflichtet hat, Kundendaten (einschließlich aller personenbezogenen Daten) für bestimmte Onlinedienste von Unternehmen zu speichern und zu verarbeiten. Die EU-Datengrenze verwendet Microsoft-Rechenzentren, die in Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Italien, den Niederlanden, Norwegen, Österreich, Polen, Schweden, der Schweiz und Spanien angekündigt wurden oder derzeit in Betrieb sind. In Zukunft kann Microsoft Rechenzentren in weiteren Ländern in der EU oder EFTA einrichten, um EU Data Boundary Services bereitzustellen.

Es gibt einige Ausnahmen von der EU-Datengrenze, die dazu führen können, dass Microsoft Kundendaten (einschließlich personenbezogener Daten) außerhalb der EU-Datengrenze verarbeitet. In diesem Fall verlässt sich Microsoft auf konforme Datenübertragungsmechanismen, wie sie in der DSGVO festgelegt sind. Weitere Einzelheiten zu diesen eingeschränkten Umständen finden Sie in den Microsoft Product Terms.

Erfahren Sie mehr über die EU-Datengrenze.

In Teil 3 erfahren Sie mehr über die Datenresidenz für Microsoft 365 Copilot.

In Teil 4 erfahren Sie mehr über die Datenresidenz für Azure OpenAI Service.



[6] Für Kunden in Großbritannien erlaubt die UK GDPR die Übermittlung personenbezogener Daten in ein Drittland außerhalb des United Kingdom (einschließlich der USA), wenn bestimmte Bedingungen erfüllt sind. Zu diesen Bedingungen gehört, wenn ein Angemessenheitsbeschluss des britischen Außenministers vorliegt oder wenn geeignete zusätzliche Garantien (wie z. B. der Nachtrag zur internationalen Datenübermittlung zu den Standardvertragsklauseln der EU-Kommission („UK Addendum") eingeführt wurden.

Wie interagiert die DSGVO mit dem AI Act?

Die DSGVO und der AI Act sollen sich ergänzen und nebeneinander wirken und einen regulatorischen Rahmen für KI-Produkte und -Dienste bieten. Die DSGVO, die die Verarbeitung personenbezogener Daten durch Verantwortliche und Datenverarbeiter regelt, konzentriert sich auf den Datenschutz und zielt darauf ab, dem Einzelnen die Kontrolle über seine personenbezogenen Daten zu geben.

Der AI Act, das für Anbieter, Importeure, Vertreiber, Nutzer und andere am KI-Lebenszyklus beteiligte Personen gilt, soll sicherstellen, dass KI-Systeme, die in der EU eingesetzt werden, die Grundrechte, die Sicherheit und die ethischen Grundsätze achten und bestimmte Risiken im Zusammenhang mit den leistungsfähigsten „General Purpose"-KI-Modellen adressieren.

Erfahren Sie in Anhang 2: Häufig gestellte Fragen (FAQs) mehr über den AI Act und sein Zusammenspiel mit der DSGVO.

Unsere kontinuierliche Compliance mit Datenschutzbestimmungen und der offene Dialog mit den wichtigsten Regulierungsbehörden in Europa und der ganzen Welt

Mit der Weiterentwicklung der Datenschutzgesetze entwickeln sich die Normen und Anforderungen in Europa und auf der ganzen Welt weiter. Sie können sicher sein, dass Microsoft in Bezug auf unsere Datenschutz- und Sicherheitspraktiken transparent ist. Wir werden uns an die Gesetze in Europa und weltweit halten, die KI regeln, und unsere Versprechen mit klaren vertraglichen Verpflichtungen untermauern.

Neben der Einhaltung der DSGVO und anderer für uns geltender gesetzlicher Anforderungen legt Microsoft Wert auf einen offenen Dialog mit seinen Kunden, Partnern und Aufsichtsbehörden, um die sich entwickelnden Bedenken hinsichtlich des Datenschutzes besser zu verstehen und zu berücksichtigen.

Wir arbeiten weiterhin eng mit Datenschutzbehörden und Datenschutzbehörden auf der ganzen Welt zusammen, um Informationen über die Funktionsweise unserer KI-Systeme auszutauschen und so ein Umfeld des Vertrauens und der Zusammenarbeit zu fördern.

Teil 3

Microsoft 365 Copilot

Die Grundlage für die DSGVO-Compliance ist ein umfassendes Verständnis dessen, welches Potenzial generative KI-Dienste bieten und wie sie funktionieren – und wie personenbezogene Daten durch diese Produkte und Services genutzt werden. Dieser dritte Teil enthält Informationen und Links zu verschiedenen externen Ressourcen, die Ihnen helfen, die Funktionsweise von Microsoft 365 Copilot zu verstehen, und bietet wichtige Informationen über das Produkt und seine Funktionen, die verwendet werden können, um eine DSFA oder eine andere Datenschutzbewertung/-analyse zu unterstützen.

Was ist Microsoft 365 Copilot und wie funktioniert es?

Microsoft 365 Copilot ist ein KI-gestütztes Produktivitätstool, das Large Language Models (LLMs) verwendet und in beliebten Microsoft 365-Anwendungen wie Word, Excel, PowerPoint, Outlook, Teams und mehr genutzt werden kann. Microsoft 365 Copilot bietet intelligente Unterstützung in Echtzeit, die es Benutzenden ermöglicht, ihre Kreativität, Produktivität und Skills zu verbessern.

Microsoft 365 Copilot basiert auf der gleichen Cloud-Infrastruktur wie die Microsoft 365-Anwendungen und wendet im Hinblick auf Vertraulichkeit und Datenschutz die gleichen Prinzipien an. Microsoft 365 Copilot entspricht allen bestehenden Datenschutz-, Sicherheits- und Compliance-Verpflichtungen, die für Microsoft 365 gelten, einschließlich der DSGVO-Verpflichtungen von Microsoft, wie sie im Data Protection Addendum und in Bezug auf die EU-Datengrenze dargelegt sind.

Microsoft 365 Copilot greift auf die organisationsbezogenen Inhalte in Ihrer Microsoft 365-Instanz zu, einschließlich der Kalender, E-Mails, Chats, Dokumente, Besprechungen, Kontakte und mehr der Benutzenden – allerdings nur entsprechend den vorhandenen Zugriffsberechtigungen. Der Umfang der Copilot-Umgebung für Microsoft 365 hängt von den Datenquellen ab, die von Microsoft 365 indiziert werden. Kunden mit den umfangreichsten Daten in Microsoft 365 (Exchange, OneDrive, SharePoint, Teams) erhalten die besten Ergebnisse mit Copilot. Durch den Zugriff auf umfassende Unternehmensdaten kann Copilot relevantere und besser personalisierte Inhalte vorschlagen, die auf dem Arbeitskontext und den Vorlieben des jeweiligen Nutzers basieren.

Copilot reagiert auf Prompts Ihrer Benutzenden. „Prompt" ist der Begriff, mit dem beschrieben wird, wie Sie Microsoft 365 Copilot bitten, etwas für Sie zu tun – z. B. Erstellen, Zusammenfassen, Bearbeiten oder Transformieren. Stellen Sie sich Prompts so vor, als würden Sie ein Gespräch führen, in einer einfachen, aber klaren Sprache und versehen mit Kontextinformationen, wie Sie es mit einem Assistenten tun würden.

Wenn Microsoft 365 Copilot Inhalte aus der Microsoft 365-Instanz der Organisation verwendet, um den Prompt des Benutzers zu erweitern und die Antwort anzureichern, wird dies als „Grounding" bezeichnet. Grounding ist etwas anderes als Training. Es werden keine Kundendaten verwendet, um das LLM zu trainieren. Tatsächlich ist das LLM „stateless", was bedeutet, dass es weder Informationen über den Prompt, der ihm übermittelt wurde, noch Kundendaten, die für das Grounding verwendet wurden, noch Antworten, die es gegeben hat, speichert.

Microsoft 365 Copilot nutzt eine Instanz eines Foundation-LLM, das in Azure OpenAI gehostet wird. Microsoft 365 Copilot interagiert nicht mit Diensten, die von OpenAI betrieben werden (z. B. ChatGPT oder die OpenAI-API). OpenAI ist kein Unterauftragsverarbeiter von Microsoft, und Kundendaten – einschließlich der Daten, die durch die Nutzung von Microsoft 365 Copilot in Ihrer Organisation generiert werden, wie Prompts und Antworten – werden ohne Ihre Erlaubnis nicht an Dritte weitergegeben.

Microsoft 365 Copilot ist

- **konzipiert** auf Basis des umfassenden Ansatzes von Microsoft in Bezug auf Sicherheit, Compliance und Datenschutz.
- **entwickelt** für den Schutz von Instanzen-, Gruppen- und individuellen Daten entwickelt.
- **ausgerichtet** auf verantwortungsvolle KI.

Verschaffen Sie sich einen Einblick in die Funktionsweise von LLMs, wenn Sie sie mit Ihren Daten in Microsoft 365 verwenden. Erfahren Sie mehr über Microsoft 365 Copilot.

Erfahren Sie im Copilot Lab, wie Copilot in Ihren bevorzugten Microsoft-Anwendungen verwendet werden kann.

Ausführlichere Informationen zu Microsoft 365 Copilot finden Sie auch auf unserem Learn-Portal.

Copilot und Ihr Datenschutz

Copilot in Windows

Erfahren Sie mehr darüber, wie Copilot Ihre Daten verwendet, um Sie auf Ihrem Windows-Gerät zu unterstützen.

Mehr zu Ihren Daten und dem Datenschutz ›

Copilot Pro (Privatanwender)

Erfahren Sie mehr darüber, wie Copilot Ihre Daten in Microsoft 365-Anwendungen verwendet.

Mehr zu Microsoft 365-Apps und Ihrer Privatsphäre ›

Microsoft 365 Copilot (IT-Experten/Administratoren)

Erfahren Sie mehr darüber, wie Ihre Organisationsdaten verwendet und geschützt werden, wenn Sie Copilot mit Microsoft 365 verwenden.

Mehr zu Daten, Datenschutz und Sicherheit ›

Wie werden personenbezogene Daten in Microsoft 365 Copilot genutzt?

Ein wichtiger Nutzen von Microsoft 365 Copilot besteht darin, dass es die LLMs von Microsoft mit Ihren Organisationsdaten verbindet. Dafür wird auf Inhalte und Kontextinformationen zugegriffen, um Antworten zu generieren, die in Ihren Organisationsdaten verankert sind, z. B. in Benutzerdateien, E-Mails, Kalendereinträgen, Chats, Besprechungen und Kontakten. Microsoft 365 Copilot kombiniert diese Inhalte mit dem Arbeitskontext des Benutzers, z. B. einer Besprechung, einem E-Mail-Verlauf zu einem bestimmten Thema oder Chatunterhaltungen, die der Benutzer in einem bestimmten Zeitraum geführt hat. Microsoft 365 Copilot verwendet diese Kombination aus Inhalt und Kontext, um für die Prompts des Benutzers genaue, relevante und kontextbezogene Antworten bereitzustellen.

Microsoft 365 Copilot kann bei Prompts auch Webinhalte aus der Bing-Suche nutzen, um Antworten zu ermitteln. Basierend auf dem Prompt des Benutzers bestimmt Microsoft 365 Copilot, ob Bing zum Abfragen von Webinhalten verwendet werden muss, um eine relevante Antwort zu generieren. Es stehen Steuerelemente für Administratoren zur Verfügung, um die Verwendung von Webinhalten zu verwalten.

Die Missbrauchsüberwachung für Microsoft 365 Copilot erfolgt in Echtzeit, ohne dass Microsoft ständigen Zugriff auf Kundendaten erhält, weder für menschliche noch für automatisierte Überprüfungen. (Die Missbrauchsmoderation für Azure OpenAI Service, die eine menschliche Überprüfung von Inhalten umfasst, ist bei Microsoft 365 Copilot nicht erforderlich.)

Microsoft sammelt und speichert Daten über Benutzerinteraktionen mit Microsoft 365 Copilot. Dazu zählen der Prompt des Benutzers, die Antwort von Copilot und die Informationen, die verwendet werden, um die Antwort von Copilot zu begründen („Content-Interaktionen"). Administratoren können die Content-Interaktionen Ihrer Organisation einsehen, verwalten und durchsuchen. Es kann erforderlich sein, Ihre Datenschutzhinweise für die Benutzer in Ihrer Organisation zu aktualisieren, um sicherzustellen, dass die Verarbeitung personenbezogener Daten durch Administratoren in diesem Zusammenhang angemessen erfasst wird. Weitere Einzelheiten zu den Transparenzpflichten im Rahmen der DSGVO finden Sie in Teil 2.

Für Microsoft ist es wichtig, dass das Eigentum an den Daten unserer Kunden bei unseren Kunden liegt. Microsoft erhebt keinen Anspruch auf das Eigentum an den Inhalten, die von Microsoft 365 Copilot erstellt wurden. Alle Content-Interaktionen, einschließlich Prompts und jeglicher Output/Content, gelten gemäß unseren Product Terms und dem Data Protection Addendum als „Kundendaten".

Alle Kundendaten, die von Microsoft 365 Copilot verarbeitet werden, werden in Übereinstimmung mit vertraglichen Verpflichtungen mit den anderen Inhalten Ihrer Organisation in Microsoft 365 verarbeitet und gespeichert.

Microsoft 365 Copilot verwendet keine Kundendaten, um Foundation-Modelle ohne die Erlaubnis der Kunden zu trainieren.

Sicherheit für Microsoft 365 Copilot

Wie in Teil 2 dargelegt, verlangt die DSGVO von den für die Verarbeitung Verantwortlichen und den Datenverarbeitern, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein definiertes Maß an Sicherheit für die von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten.

Für Microsoft 365 Copilot gelten standardmäßig dieselben Sicherheits- und Compliance-Bestimmungen, die bereits für die Nutzung von Microsoft 365 in Ihrer Organisation gelten. Microsoft 365 Copilot wird in einer Azure-Infrastruktur gehostet und durch einige der branchenweit umfassendsten Compliance- und Sicherheitsmaßnahmen geschützt. Bei der Entwicklung von Microsoft 365 Copilot wurde die Nutzung der gleichen Sicherheits- und Compliance-Funktionen festgelegt, die in der Hyperscale-Cloud von Microsoft bereits gut etabliert sind. Dazu zählen Zuverlässigkeit, Redundanz, Verfügbarkeit und Skalierbarkeit, die alle standardmäßig in unsere Cloud-Services integriert sind.

Microsoft 365 Copilot berücksichtigt auch die Zugriffsberechtigungen jedes Benutzers auf alle Inhalte, die abgerufen werden. Dies ist wichtig, da Microsoft 365 Copilot nur Antworten generiert, die auf Informationen basieren, für die der jeweilige Benutzer die Berechtigung hat.

Microsoft implementiert mehrere Schutzmaßnahmen, um zu verhindern, dass Kunden Microsoft 365-Dienste und -Anwendungen kompromittieren oder unbefugten Zugriff auf andere Instanzen oder das Microsoft 365-System selbst erhalten.

Im Folgenden finden Sie einige Beispiele für diese Schutzmaßnahmen

- Die logische Isolierung von Kundendaten innerhalb jeder Instanz für Microsoft 365-Dienste wird durch die Autorisierung und rollenbasierte Zugriffssteuerung von Microsoft Entra erreicht. Erfahren Sie mehr über Microsoft 365-Isolationssteuerungen.
- Microsoft setzt auf strenge physische Sicherheit, Hintergrundüberprüfungen und eine mehrschichtige Verschlüsselungsstrategie, um die Vertraulichkeit und Integrität von Kundendaten zu schützen.
- Microsoft 365 nutzt dienstseitige Technologien, die Kundendaten sowohl im Ruhezu-stand als auch während der Übertragung („at Rest" und „in Transit") verschlüsseln, darunter BitLocker, Verschlüsselung pro Datei, Transport Layer Security (TLS) und Internet Protocol Security (Ipsec).

  Weitere Informationen zur Verschlüsselung in Microsoft 365 finden Sie unter Verschlüsselung in der Microsoft Cloud.
- Ihre Kontrolle über die Daten Ihrer Organisation wird durch die Verpflichtung von Microsoft verstärkt, allgemein geltende Datenschutzgesetze einzuhalten, einschließlich der DSGVO und Datenschutzstandards wie ISO/IEC 27018.
- Bei Inhalten, auf die über Microsoft 365 Copilot-Plug-ins zugegriffen wird, kann die Verschlüsselung den programmatischen Zugriff ausschließen, wodurch das Plug-in im auf die Inhalte eingeschränkt wird.
- Da generative KI-Systeme auch Softwaresysteme sind, gelten alle Elemente unseres Security Development Lifecycle: von der Bedrohungsmodellierung über die statische Analyse, den sicheren Aufbau und Betrieb bis hin zur Verwendung starker Kryptografie, Identitätsstandards und mehr.
- Unser Security Development Lifecycle wurde zudem um weitere Schritte ergänzt, um uns auf KI-Bedrohungsvektoren vorzubereiten, einschließlich der Aktualisierung der SDL-Anforderung für die Bedrohungsmodellierung, um KI- und Machine-Learning-spezifische Bedrohungen zu berücksichtigen. Wir unterziehen unsere KI-Produkte einem AI-Red-Teaming, um Schwachstellen zu ermitteln und sicherzustellen, dass wir über geeignete Strategien zur Risikominderung verfügen.

EU-Datengrenze und Datenresidenz

Wie in Teil 2 dieses Leitfadens erläutert, handelt es sich bei Microsoft 365 Copilot um einen EU Data Boundary Service.

Erfahren Sie mehr über die EU-Datengrenze.

Wenn Sie von Copilot generierte Daten in Microsoft 365-Produkten speichern, für die bereits Verpflichtungen zur Datenresidenz gemäß den Product Terms gelten, greifen die anwendbaren Verpflichtungen.

Microsoft 365 Copilot wurde als abgedeckter Workload in den Verpflichtungen zur Datenresidenz in den Microsoft Product Terms aufgenommen. Die Angebote zu Microsoft Advanced Data Residency und Multi-Geo umfassen ebenfalls Verpflichtungen zur Datenresidenz für Microsoft 365 Copilot-Kunden.

Teil 4

Azure OpenAI Service

Was ist der Azure OpenAI Service und wie funktioniert er?

Azure OpenAI Service ist eine cloudbasierte Plattform, auf der Kunden ihre eigenen generativen KI-Anwendungen erstellen und bereitstellen können, indem sie die Leistungsfähigkeit von KI-Modellen nutzen. Azure OpenAI Service bietet Kunden Zugriff auf eine Reihe von LLMs für die Entwicklung von generativen KI-Erfahrungen.

Von der Generierung realistischer Bilder und Videos bis hin zur Verbesserung von Kundenerlebnissen hat sich generative KI in verschiedenen Branchen als vielseitiges Werkzeug erwiesen. Die Modelle, die dem Azure OpenAI Service zugrundeliegen, können problemlos an Ihre spezifische Aufgabe angepasst werden, einschließlich: Gestaltung, Erstellung und Generierung von Inhalten, Zusammenfassungen, semantische Suche, Übersetzung von natürlicher Sprache in Code, beschleunigte Automatisierung, personalisiertes Marketing, Chatbots und virtuelle Assistenten, Produkt- und Serviceinnovationen, Sprachübersetzung und Verarbeitung natürlicher Sprache, Betrugserkennung und Cybersicherheit, Predictive Analytics und Prognosen, kreatives Schreiben sowie medizinische Forschung und Diagnosestellung.

Der Azure OpenAI Service wird vollständig von Microsoft gesteuert. Microsoft hostet die OpenAI-/ChatGPT-Modelle in der Azure-Umgebung von Microsoft und der Dienst interagiert nicht mit Diensten, die von OpenAI betrieben werden (z. B. ChatGPT oder die OpenAI-API).

OpenAI/ChatGPT besitzt und trainiert die Foundation-LLMs, die Microsoft verwendet, und Microsoft hat eine Lizenz, Dienste anzubieten, die auf diesen Foundation-LLMs basieren.

OpenAI/ChatGPT ist kein Unterauftragsverarbeiter von Microsoft, und Kundendaten – einschließlich der Daten, die durch die Nutzung des Azure OpenAI Service in Ihrer Organisation generiert werden, wie Prompts und Antworten – werden privat gehalten und ohne Ihre Erlaubnis nicht an Dritte weitergegeben.

Erfahren Sie mehr über die zugrundeliegenden LLMs, die den Azure OpenAI Service unterstützen.

Der Azure OpenAI Service kann auf folgende Weise verwendet werden:

- **Prompt Engineering:** Prompt Engineering ist eine Technik, bei der Prompts für LLMs entworfen werden. Prompts werden vom Benutzer übermittelt, und der Dienst generiert Inhalte über Vorgänge wie Vervollständigungen, Chatvervollständigungen, Bilder und Einbettung. Dieser Prozess verbessert die Genauigkeit und Relevanz von Antworten und optimiert die Leistung des Modells.

  Erfahren Sie mehr über Prompt Engineering.

- **Azure OpenAI On Your Data:** Wenn Sie das Feature „On Your Data" verwenden, ruft der Dienst relevante Daten aus einem konfigurierten Kundendatenspeicher ab und erweitert den Prompt, um Generierungen zu erstellen, die auf Ihren Daten basieren.

  Mit Azure OpenAI „On Your Data" können Sie unterstützte LLMs für die Daten Ihrer Organisation ausführen, ohne Modelle trainieren oder optimieren zu müssen. Das Ausführen von Modellen für Kundendaten ermöglicht es Ihnen, Ihre Daten mit größerer Genauigkeit und Geschwindigkeit zu analysieren. Auf diese Weise können Sie wertvolle Insights gewinnen, die Ihnen helfen können, bessere Entscheidungen zu treffen, Trends und Muster zu erkennen und Ihre Abläufe zu optimieren.

  Einer der Hauptvorteile von Azure OpenAI „On Your Data" ist die Möglichkeit, den Inhalt von Conversational AI anzupassen. Das Modell innerhalb von Azure OpenAI Service hat Zugriff auf bestimmte Quellen und kann auf diese referenzieren, um Antworten zu unterstützen. Die Antworten basieren nicht nur auf seinem vortrainierten Wissen, sondern auch auf den neuesten Informationen, die in der angegebenen Datenquelle verfügbar sind. Diese Grounding-Daten helfen dem Modell auch, zu vermeiden, dass Antworten auf der Grundlage veralteter oder falscher Informationen generiert werden.

  Erfahren Sie mehr über Azure OpenAI für Ihre Daten.

- **Azure OpenAI-Feinabstimmung:** Sie können Ihre eigenen Trainingsdaten bereitstellen, die aus Prompt-Vervollständigungspaaren bestehen, um ein OpenAI-Modell feiner abzustimmen und so zu optimieren. Bei diesem Prozess wird ein vorhandenes LLM anhand von Beispieldaten verfeinert. Diese Feinabstimmung bezieht sich auf den Prozess des erneuten Trainings von vortrainierten Modellen für bestimmte Datasets, in der Regel, um die Modellleistung bei bestimmten Aufgaben zu verbessern oder Informationen zu ergänzen, die beim ursprünglichen Training des Basismodells nicht gut repräsentiert waren. Das Ergebnis ist ein neues eigenes LLM („Custom LLM"), das anhand der bereitgestellten Beispiele für den Kunden optimiert wurde.

Trainingsdaten und fein abgestimmte Modelle

1. sind ausschließlich für die Verwendung durch Ihre Organisation verfügbar.
2. werden in derselben Region wie die Azure OpenAI-Ressource gespeichert.
3. können vom Kunden jederzeit gelöscht werden.

Wenn Sie eigene Daten hochladen, um die Ergebnisse des LLM zu optimieren, werden sowohl die Kundendaten als auch die Ergebnisse des fein abgestimmten Modells in einem geschützten Bereich der Cloud verwaltet, der in Ihrer Instanz gespeichert wird – nur für Ihre Organisation zugänglich und durch robuste Kontrollmechanismen getrennt, um jeden anderen Zugriff zu verhindern. Die Kundendaten und -ergebnisse können zusätzlich mit entweder von Microsoft oder vom Kunden verwalteten Verschlüsselungsschlüsseln in einem Bring Your Own Key-Format verschlüsselt werden, wenn ein Kunde dies wünscht. In den meisten Fällen kann Microsoft Probleme mit dem Dienst unterstützen und beheben, ohne Zugriff auf Kundendaten zu benötigen (z. B. die Daten, die zur Feinabstimmung hochgeladen wurden). In den seltenen Fällen, in denen Zugriff auf Kundendaten erforderlich ist, sei es zur Bearbeitung eines vom Kunden initiierten Supporttickets oder zur Behebung eines von Microsoft identifizierten Problems, können Sie die Kontrolle über den Zugriff auf diese Daten mithilfe der Customer Lockbox für Microsoft Azure übernehmen. Diese Lockbox gibt Kunden die Möglichkeit, Zugriffsanfragen auf ihre Kundendaten zu genehmigen oder abzulehnen.

Erfahren Sie mehr über die Azure OpenAI-Optimierung.

Unabhängig davon, ob Inhalte verwendet werden, um Prompts mithilfe der Funktion „On Your Data" zu grounden oder ein Feinabstimmungsmodell zu erstellen, werden die Kundendaten nicht zum Trainieren des grundlegenden LLM verwendet. Tatsächlich ist das LLM „stateless", was bedeutet, dass er weder Informationen über den Prompt, der ihm übermittelt wurde, noch Kundendaten, die für das Grounding verwendet wurden, noch Antworten, die er gegeben hat, speichert. Das LLM wird nicht trainiert und lernt zu keinem Zeitpunkt während dieses Prozesses; sondern es ist genau das gleiche grundlegende Modell, auch wenn es von Millionen von Prompts durchlaufen wurde.

Ausführliche Informationen zu Azure OpenAI Service finden Sie in der Azure OpenAI Service-Dokumentation.

Prävention von Missbrauch und Generierung schädlicher Inhalte

Um das Risiko einer schädlichen Nutzung von Azure OpenAI Service zu verringern, sind sowohl Funktionen für die Filterung von Inhalten als auch die Überwachung auf Missbrauch enthalten.

Bei der Content-Filterung werden Antworten automatisiert synchron untersucht, um zu bestimmen, ob sie gefiltert werden sollten, bevor sie an einen Benutzer zurückgegeben werden. Diese Untersuchung erfolgt ohne die Notwendigkeit, Daten zu speichern, und ohne menschliche Überprüfung der Prompts (d. h. des Textes, der von Benutzern als Anfrage eingegeben wird) oder der Antworten (d. h. der Daten, die an den Benutzer zurückgegeben werden).

Erfahren Sie mehr über die Content-Filterung.

Die Überwachung auf Missbrauch erfolgt in einem separaten Prozess. Auf diese Daten darf nur autorisiertes Microsoft-Personal zugreifen, um das Debuggen zu unterstützen und vor Missbrauch des Systems zu schützen. Hierbei handelt es sich um autorisierte Microsoft-Mitarbeitende, die über punktuelle Abfragen mithilfe von Request-IDs, Secure Access Workstations (SAWs) und Just-in-Time-Anforderungsgenehmigungen (JIT), die von Vorgesetzten erteilt werden, auf die Daten zugreifen.

Erfahren Sie mehr über die Überwachung auf Missbrauch.

Diese menschliche Überprüfung kann eine Herausforderung für Kunden darstellen, die ein Gleichgewicht zwischen der Sicherheit des Systems und den Risiken externen Zugriffs finden müssen – selbst unter kontrollierten Bedingungen. Dafür bietet Microsoft Funktionen mit eingeschränktem Zugriff, um diese menschlichen Überprüfungs- und Datenprotokollierungsprozesse in genehmigten Kunden-Use-Cases ablehnen zu können.

Einige Kunden möchten Azure OpenAI Service möglicherweise für einen Use-Case verwenden, der die Verarbeitung vertraulicher, streng vertraulicher oder gesetzlich regulierter Input-Daten umfasst, bei dem jedoch die Wahrscheinlichkeit von schädlichem Output und/oder Missbrauch gering ist. Möchte ein solcher Kunde aufgrund ihrer internen Richtlinien oder des geltenden Rechts ausschließen, dass Microsoft die entsprechenden Daten zur Missbrauchserkennung verarbeiten kann, kann er bei Microsoft die Deaktivierung der Content-Management-Funktionen von Azure OpenAI Service beantragen. Dafür muss dieses Formular ausgefüllt werden.

Wird diese Deaktivierung durch Microsoft bestätigt, werden für dieses Azure-Abonnement keine keine Prompts und Vervollständigungen im Sinne der Missbrauchsüberwachung gespeichert. Somit ist kein menschlicher Überprüfungsprozess möglich und wird nicht ausgeführt.

Wie werden personenbezogene Daten in Azure OpenAI Service genutzt?

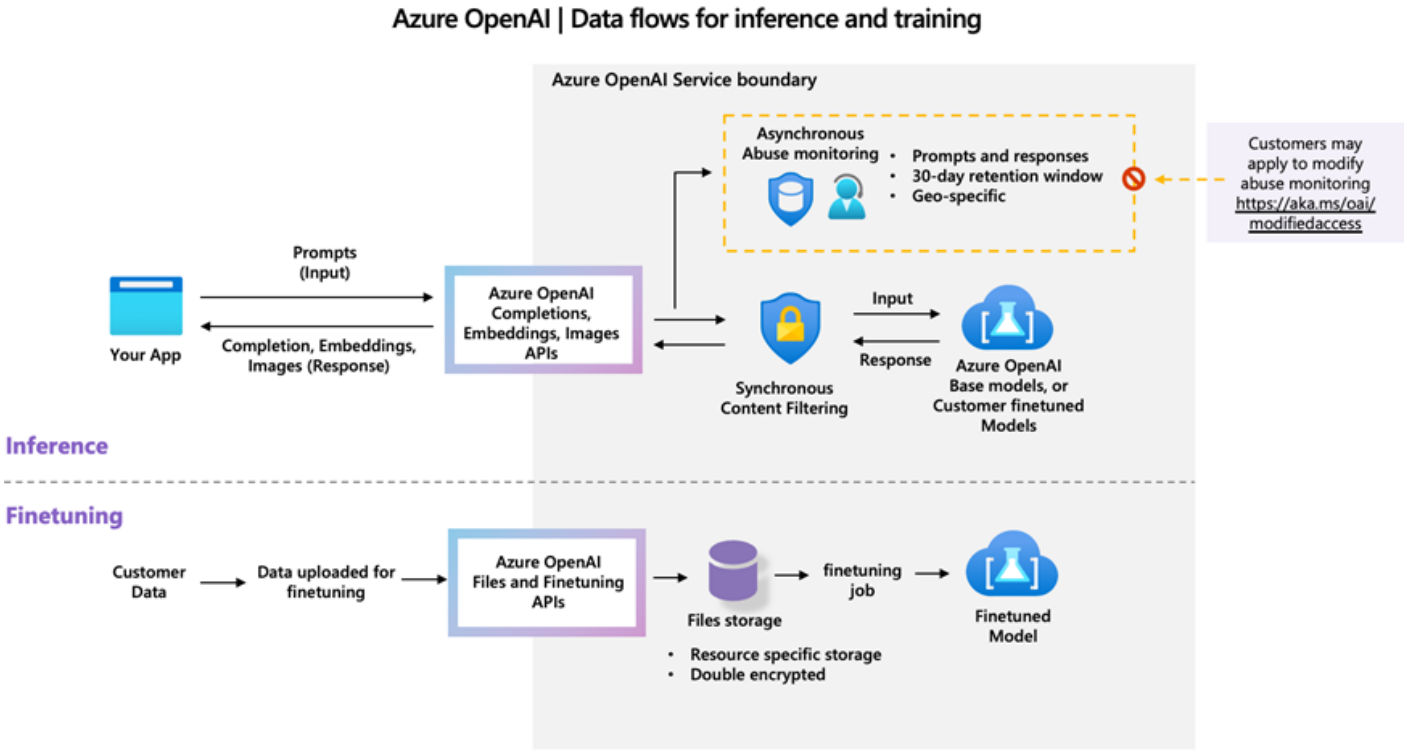
Das untenstehende Diagramm veranschaulicht, wie die Daten Ihrer Organisation vom Azure OpenAI Service verarbeitet werden. Dieses Diagramm deckt drei verschiedene Arten der Verarbeitung ab:

1. Wie Azure OpenAI Service Ihre Prompts verarbeitet, um **Inhalte zu generieren** (z. B. wenn einem Prompt mithilfe von Azure OpenAI „On Your Data" zusätzliche Daten aus einer verbundenen Datenquelle hinzugefügt werden)
2. Wie Azure OpenAI Service **ein fein abgestimmtes, eigenes („Custom") Modell** mit Ihren Trainingsdaten erstellt
3. Wie Azure OpenAI Service und Microsoft-Mitarbeitende Prompts, Vervollständigungen und Bilder auf schädliche Inhalte und auf Muster **analysieren**, die auf die Verwendung des Diensts in einer Weise hindeuten, die gegen den Verhaltenskodex oder andere geltende Produktbedingungen verstößt.

Kunden-Prompts (Input/Eingaben) und Vervollständigungen (Output), Einbettungen und Trainingsdaten:

- stehen **anderen Kunden** NICHT zur Verfügung.
- stehen **OpenAI** NICHT zur Verfügung.
- werden NICHT verwendet, um **Foundation-Modelle** ohne die Erlaubnis des Kunden zu trainieren.
- werden NICHT verwendet, um **Produkte oder Dienste von Microsoft oder Drittanbietern** zu verbessern.
- werden NICHT zum **automatischen Verbessern von Azure OpenAI-Modellen** für die Verwendung in Ihrer Ressource verwendet. (Die Modelle sind „stateless", es sei denn, Sie stimmen die Modelle explizit mit Ihren Trainingsdaten feiner ab.)

Von Kunden feinabgestimmte Azure OpenAI-Modelle sind exklusiv für die Verwendung in Ihrer Organisation verfügbar.



Sicherheit für Azure OpenAI

Wie in Teil 2 dargelegt, verlangt die DSGVO von Datenverantwortlichen und Datenverarbeitern, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein Sicherheitsniveau für alle von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten.

Sicherheit ist entlang des gesamten Entwicklungslebenszyklus aller unserer Enterprise-Services (einschließlich derjenigen, die generative KI-Technologie beinhalten) integriert, von der Konzeptionierung bis zur Bereitstellung.

Azure OpenAI Service wird in der Azure-Infrastruktur gehostet und durch einige der umfassendsten Compliance- und Sicherheitskontrollen für Unternehmen in der Branche geschützt. Diese Dienste wurden entwickelt, um die Sicherheits- und Compliance-Funktionen zu nutzen, die in der Hyperscale-Cloud von Microsoft bereits gut etabliert sind. Dazu gehört die Priorisierung von Zuverlässigkeit, Redundanz, Verfügbarkeit und Skalierbarkeit, die alle standardmäßig in unsere Cloud-Services integriert sind.

Da generative KI-Systeme auch Softwaresysteme sind, gelten alle Elemente unseres Security Development Lifecycle: von der Bedrohungsmodellierung über die statische Analyse, den sicheren Aufbau und Betrieb bis hin zur Verwendung starker Kryptografie, Identitätsstandards und mehr.

Wir haben auch neue Schritte zu unserem Security Development Lifecycle hinzugefügt, um uns auf KI-Bedrohungsvektoren vorzubereiten, einschließlich der Aktualisierung der SDL-Anforderung für die Bedrohungs-modellierung, um KI- und Machine Learning-spezifische Bedrohungen zu berücksichtigen. Wir unterziehen unsere KI-Produkte einem KI-Red-Teaming, um nach Schwachstellen zu suchen und zu bestätigen, dass wir über geeignete Strategien zur Risikominderung verfügen.

Erfahren Sie mehr über Datenschutz und Sicherheit für Azure OpenAI Service.

EU-Datengrenze und Datenresidenz

Azure OpenAI Service ist ein EU Data Boundary Service. Im Sinne des Abschnitts „EU Data Boundary Services" in den Product Terms ist Azure OpenAI Service ein Azure-Dienst, der die Bereitstellung in einer Region innerhalb der EU-Datengrenze ermöglicht.

Erfahren Sie mehr über die EU-Datengrenze.

Dabei gelten folgende Besonderheiten:

- **Azure OpenAI On Your Data-Funktion:** Alle Datenquellen, die Sie bereitstellen, um die generierten Ergebnisse zu grounden, bleiben in der von Ihnen angegebenen Datenquelle und am von Ihnen angegebenen Speicherort gespeichert. Es werden keine Daten in den Azure OpenAI Service kopiert.
- **Trainingsdaten und fein abgestimmte („Custom") LLMs:** Diese werden in derselben Region wie die Azure OpenAI-Ressource in der Azure-Instanz des Kunden gespeichert.
- **Missbrauchsüberwachung für Kunden, die Azure OpenAI Service in Europa nutzen:** Diese Überprüfung wird ausschließlich von Microsoft-Mitarbeitenden im Europäischen Wirtschaftsraum (EWR) durchgeführt. Der Datenspeicher, in dem Prompts und Outputs gespeichert werden, ist logisch nach Kundenressource getrennt (und jeder Request enthält die Ressourcen-ID der Azure OpenAI-Ressource des Kunden). In jeder Region, in der Azure OpenAI Service verfügbar ist, befindet sich ein separater Datenspeicher, und die Prompts und generierten Inhalte eines Kunden werden in der Azure-Region gespeichert, in der die Azure OpenAI Service-Ressource des Kunden innerhalb der Azure OpenAI Service-Grenze bereitgestellt wird.

Teil 5

Fazit

Microsoft steht für Vertrauen. Wir setzen uns bei allem, was wir tun, für Sicherheit, Datenschutz und Compliance ein, und das gilt ebenso für unseren Ansatz bei generativer KI. Als Branchenführer in der Bereitstellung von generativen KI-Lösungen genießen wir das Vertrauen von Kunden auf der ganzen Welt und halten uns an die strengsten Datenschutz- und Sicherheitsstandards der Branche. Wir bieten unseren Kunden führende Produkte und Services und tragen so dazu bei, dass sie ihre Ziele bei der digitalen Transformation konsequent weiterverfolgen und erreichen können.

Darüber hinaus kommunizieren wir Kunden gegenüber sehr bewusst unser Commitment und unser Engagement für Datensicherheits- und Datenschutzfragen, auch und gerade im Hinblick auf die DSGVO. Dieses Engagement spiegelt sich in unseren Verträgen, in umfangreichen technischen Dokumentationen (mit Details zu unseren Datenprozessen und -aktivitäten) und in der Implementierung technischer und organisatorischer Sicherheitsvorkehrungen wider, um verbleibende Datenschutz- und Sicherheitsrisiken zu mindern. Dies wird durch eine konsequente Zusammenarbeit mit regulatorischen und branchenspezifischen Stakeholdern unterstützt, mit denen wir eng an Zielen wie Verantwortung, Rechenschaftspflicht und Integrität bei der Bereitstellung generativer KI-Lösungen zusammenarbeiten.

Da sich sowohl das regulatorische Umfeld als auch unsere KI-Innovationen beständig weiterentwickeln, sind wir uns unserer Vorreiterstellung bei der Umsetzung neuer Datenschutzanforderungen bewusst. Microsoft wird auch künftig branchenführende Tools, Ressourcen für höchste Transparenz und Support bieten – und wir werden weiterhin unser anhaltendes Engagement unter Beweis stellen, um unsere Kunden bei der Erfüllung ihrer Bedürfnisse und Anforderungen rund um den Einsatz von KI bestmöglich zu unterstützen.

Anhang 1

Geschäftschancen, die mit generativer KI entstehen

Die Verfügbarkeit von generativen KI-Lösungen hat sich als Motor für eine Vielzahl von Use-Cases erwiesen. Im Folgenden stellen wir einige interessante Praxisbeispiele vor.

Chancen für eine Transformation mit KI

Mit der Einbindung von generativer KI in das Tagesgeschäft sind mehrere wichtige Chancen verbunden:

Anreicherung von Employee Experiences: Durch die Automatisierung von routinemäßigen und zeitintensiven Aufgaben erhalten Teams mehr Freiheit, um sich stärker auf strategische Initiativen zu fokussieren. KI-gesteuerte Prozesse verringern menschliche Fehler und erhöhen die Präzision der Ergebnisse – von Finanzprognosen bis hin zu Compliance-Prüfungen.

Neudefinition von Customer Experiences: Durch die Bereitstellung personalisierter Erlebnisse und durch schnellere Antworten auf Kundenanfragen kann KI dazu beitragen, die allgemeine Kundenzufriedenheit und -bindung zu verbessern.

Neugestaltung von Geschäftsprozessen: Wenn Unternehmen wachsen, kann KI problemlos skaliert werden, um ein erhöhtes Daten- und Transaktionsvolumen zu bewältigen und eine konsistent hohe Leistung zu bieten, ohne dass sich die Betriebskosten im gleichen Ausmaß erhöhen.

Förderung von Innovationen: KI erleichtert die Erforschung neuer Geschäftsmodelle und Services, da sie Sie dabei unterstützt, Trends erkennen, Marktdynamiken vorherzusagen und Angebote anzupassen.

Diese Einführung bildet die Grundlage für eine detaillierte Untersuchung von spezifischen Use-Cases mit generativer KI in verschiedenen Branchen und zeigt auf, wie Sie ihr Potenzial in praktische und transformative Vorteile für Ihr Unternehmen umwandeln.

Beispielhafte Ergebnisse in verschiedenen Branchen

Anreicherung von Employee Experiences

41 %

bessere Such- und Antwortqualität bei internem KI-Assistenten

KPMG

Neudefinition von Customer Experiences

24 Stunden

eingesparte Arbeitszeit pro Woche mit 24/7-Service

NHS

Neugestaltung von Geschäftsprozessen

70 %

schnellere Untersuchungen bei Finanzbetrug und -risiken

SymphonyAI

Förderung von Innovationen

98 %

Strukturvorschläge und Formatierungen durch Copilot erledigt

gm

Allgemeine Anwendungsfälle für Microsoft 365 Copilot

Microsoft 365 Copilot wurde entwickelt, um die operative Effizienz und Entscheidungsfindung in einer Vielzahl von Branchen zu verbessern. In diesem Abschnitt werden die beliebtesten universell nutzbaren Anwendungsfälle mit Microsoft 365 Copilot skizziert, um die Flexibilität und den Mehrwert für praktisch jede Organisation zu vermitteln.

- **Automatisierung im Kundensupport:** Leistungsstarke virtuelle Assistenten und Chatbots können Kundenanfragen verwalten, Echtzeit-Support bieten und Probleme autonom lösen. Dies verkürzt die Reaktionszeiten, erhöht die Kundenzufriedenheit und senkt die Betriebskosten, die sonst mit großen Kundenserviceteams verbunden sind.
- **Dokumentenautomatisierung und -verwaltung:** Mit Funktionen für das Erstellen, Formatieren und Verwalten von Dokumenten kann Copilot anhand von Benutzereingaben Berichte generieren, Korrespondenzen entwerfen und Präsentationen vorbereiten. Dies steigert die Produktivität und sorgt für Konsistenz in der gesamten Geschäftskommunikation, sodass sich die Mitarbeitenden stärker auf strategische Aufgaben konzentrieren können.
- **Datenanalysen und Generierung von Insights:** Analysieren Sie große Datensätze, um Trends zu erkennen, Predictive Analytics durchzuführen und praktische Erkenntnisse zu gewinnen, die Ihre Entscheidungsfindung unterstützen. So können Sie anhand datengestützter Einblicke den Betrieb optimieren und die strategische Planung verbessern.
- **Workflow- und Prozessautomatisierung:** Automatisieren Sie sich wiederholende und zeitintensive Aufgaben wie Dateneingabe, Terminplanung und Prozessverfolgung und profitieren Sie von nahtlos Integration in bestehende Systeme, um Arbeitsabläufe zu optimieren. Dies erhöht die operative Effizienz, reduziert menschliche Fehler und gibt den Mitarbeitenden die Möglichkeit, sich auf höherwertige Tätigkeiten zu konzentrieren.
- **Personalisierte Inhalte und Empfehlungen:** Microsoft 365 Copilot passt Inhalte und Empfehlungen für User auf der Grundlage ihres Verhaltens, ihrer Vorlieben und früheren Interaktionen an. Dies verbessert die Benutzerbindung und -zufriedenheit – und letztlich auch den Umsatz.

Abteilungs- und mitarbeiterspezifische Anwendungsfälle

In der Microsoft Copilot-Szenarienbibliothek finden Sie Anleitungen für abteilungs- und mitarbeiterspezifische Use-Cases. Nutzen Sie diese als Inspiration, um Ihre Teams zu stärken und Mehrwert Ihrer Investitionen in Microsoft 365 Copilot zu steigern.

Weitere Beispiele nach Abteilung und Rolle finden Sie unter den folgenden Links:

Use-Cases in der Finanzabteilung

Use-Cases im Personalwesen

Use-Cases im IT-Team

Use-Cases in der Marketingabteilung

Use-Cases im Vertrieb

Branchenspezifische Anwendungsfälle

In diesem Abschnitt werden spezifische Use-Cases mit Microsoft 365 Copilot in drei wichtigen Branchen vorgestellt: Rechts-, Bank- und Gesundheitswesen. Anhand dieser gezielten Beispiele wird die Effektivität von Copilot bei der Adressierung branchenspezifischer Herausforderungen und der Verbesserung des Kerngeschäfts leichter greifbar:

1. Use-Cases im Rechtswesen

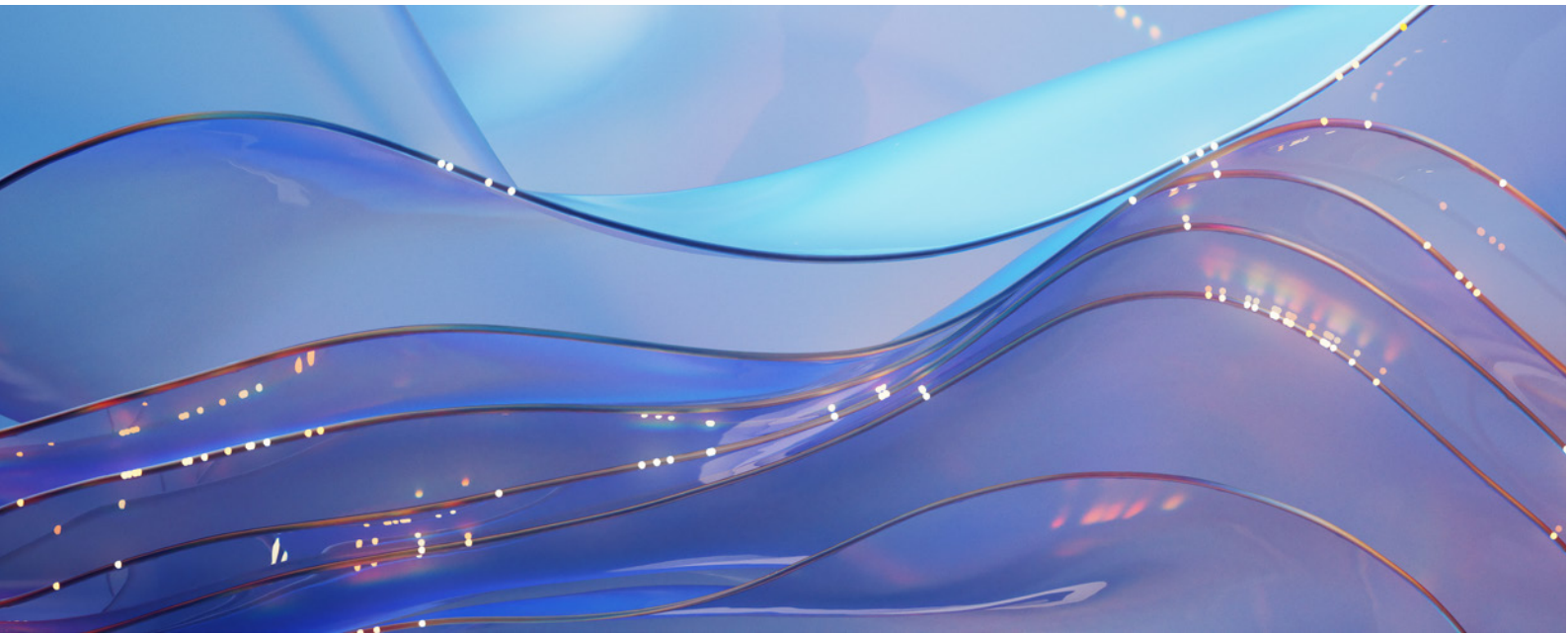
- **Vertragsprüfung und -analyse:** Automatisierung des Überprüfungsprozesses, indem Vertragsklauseln mit gesetzlichen Standards und früheren Verträgen verglichen werden. Dies erhöht die Effizienz, verringert menschliche Fehler und stellt die rechtliche Compliance sicher.
- **Unterstützung bei Rechtsstreitigkeiten:** Organisation und Analyse großer Mengen von fallbezogenen Daten, um Prozesse zeitsparend zu unterstützen und die Vorbereitung und Darlegung von rechtlichen Argumenten zu erleichtern.
- **Compliance-Überwachung:** Kontinuierliche Prüfung auf Gesetzesänderungen, damit Unternehmen relevante Gesetze einhalten. Dies reduziert das Risiko von Sanktionen und stärkt den Ruf der Kanzlei für ihre Sorgfalt.

2. Use-Cases im Bankwesen

- **Betrugserkennung:** Echtzeit-Überwachung von Transaktionen und Identifizierung von Mustern, die auf betrügerische Aktivitäten hinweisen. So lassen sich finanzielle Verluste minimieren und das Vertrauen der Kunden stärken.
- **Risikobewertung:** Analyse von Kundendaten, um potenzielle Risiken bei Kreditvergaben und Investitionen vorherzusagen und zu mindern. Dies verbessert die Fähigkeit der Bank, Risiken effektiv zu steuern.
- **Compliance-Nachverfolgung:** Ermittlung und Prüfung von regulatorischen Anforderungen um zu gewährleisten, dass die Bank die Finanzvorschriften einhält. Dadurch werden rechtliche Strafen vermieden und die betriebliche Integrität gewahrt.

3. Use-Cases im Gesundheitswesen

- **Patientendatenverwaltung:** Verwaltung und Sicherung großer Mengen an Patientendaten, sodass Gesundheitsdienstleister einen einfacheren Zugriff erhalten – für mehr Effizienz und einen höheren Vertraulichkeitsstandard in der Patientenversorgung.
- **Diagnostische Unterstützung:** Hilfe bei der Diagnose von Krankheiten durch die Analyse von Patientendaten und medizinischen Bildern. Dies erhöht die Genauigkeit der Diagnosen und die Wirksamkeit von Behandlungsplänen.
- **Remote-Patientenüberwachung:** Monitoring für Patientinnen und Patienten anhand von Daten von tragbaren Geräten und Übermittlung von Gesundheitsupdates in Echtzeit. Dies reduziert Wiedereinweisungen ins Krankenhaus und ermöglicht ein proaktives Gesundheitsmanagement.



Anhang 2

Häufig gestellte Fragen (FAQs)

Wie werden die Daten meiner Organisation geschützt, wenn ich die generativen KI-Dienste von Microsoft verwende?

Microsoft setzt auf Vertrauen, und wir engagieren uns stark für Sicherheit, Datenschutz und Compliance – auch und gerade bei unserem Ansatz für generative KI.

Datenschutz zählt zu unseren Grundsätzen, und im Sinne unseres Ansatzes für verantwortungsvolle KI vertreten wir Werte wie Datenschutz und -sicherheit, Fairness, Verantwortlichkeit, Transparenz, Inklusion sowie Zuverlässigkeit und Sicherheit, die für all unsere KI-Produkte und -Lösungen gelten.

In Teil 2 haben wir sieben Commitments skizziert, die für unser kontinuierliches Engagement für den Schutz der Daten unserer Kunden bei der Nutzung unserer generativen KI-Dienste stehen:

- Wir halten die Daten Ihres Unternehmens privat.
- Sie haben die Kontrolle über die Daten Ihrer Organisation.
- Ihre Zugriffskontrolle und Unternehmensrichtlinien werden beibehalten.
- Die Daten Ihrer Organisation werden nicht ohne Ihre Erlaubnis freigegeben.
- Der Datenschutz und die Sicherheit Ihrer Organisation sind „by Design" geschützt.
- Die Daten Ihrer Organisation werden ohne Ihre Erlaubnis nicht zum Trainieren von Foundation-Modellen verwendet.
- Unsere Produkte und Lösungen entsprechen den weltweiten Datenschutzbestimmungen.

Was ist generative KI und welche verschiedenen Arten von KI-Modellen verwendet Microsoft?

Generative KI ist eine Art von künstlicher Intelligenz, die neue Dinge wie Bilder, Text oder Sprache erstellen kann, die den Beispielen ähneln, die sie zuvor gesehen hat. Dies geschieht, indem sie aus einer Reihe von Beispielen lernt, ihre Muster und Regeln versteht und anhand dieser Muster und Regeln neue Beispiele generiert, die denen ähneln, aus denen sie gelernt hat. Sie unterscheidet sich von anderen Arten von KI, weil sie neue Dinge erschaffen kann, anstatt nur Dinge zu erkennen oder zu klassifizieren, die sie zuvor gesehen hat.

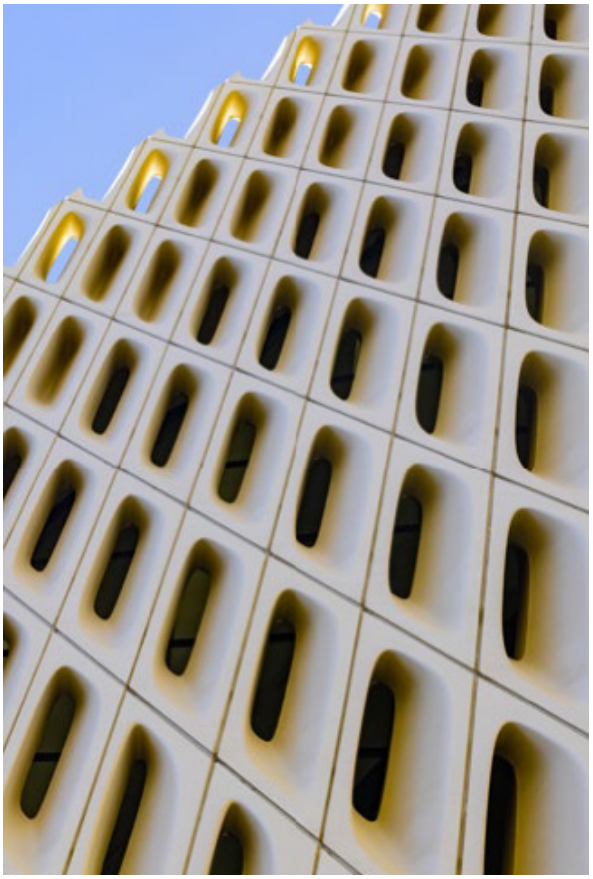
Der Azure OpenAI Service von Microsoft und Microsoft 365 Copilot ermöglichen es Kunden, die Modelle von OpenAI, einschließlich GPT-3, GPT-4 und Codex, in der Microsoft-Umgebung zu nutzen. Diese Modelle werden allgemein als „Foundation Models" bezeichnet, die als groß angelegte KI-Modelle verstanden werden, die mit riesigen Mengen von hauptsächlich ungelabelten Daten in großem Maßstab trainiert werden (in der Regel durch Self-Supervised-Lernen) und mit minimaler Feinabstimmung für eine Reihe verschiedener nachgelagerter Aufgaben angepasst werden können.

Wo liegen im Sinne der DSGVO die Unterschiede zwischen Cloud- und generativen KI-Diensten?

Die DSGVO-Verpflichtungen, die für die Nutzung von Cloud-Computing-Diensten gelten, greifen auch für die Nutzung generativer KI-Dienste. Die DSGVO verlangt bei der Implementierung und Nutzung neuer Technologien einen risikobasierten Ansatz.

Die Höhe des Risikos hängt von der Art, dem Umfang, dem Inhalt und dem Zweck ab, für den personenbezogene Daten verwendet werden. Bei der Nutzung von Cloud-Diensten und/oder generativen KI-Diensten muss ein Unternehmen prüfen, welche technischen und organisatorischen Maßnahmen zum Schutz und zur Absicherung der Nutzung personenbezogener Daten vorhanden sind, und es muss sicherstellen, dass es über angemessene vertragliche Verpflichtungen und interne Prozesse verfügt, um seinen Verpflichtungen aus der DSGVO nachzukommen.

In Teil 2 dieses Leitfadens erfahren Sie mehr darüber, wie Microsoft Kunden bei der Durchführung dieser Bewertung unterstützen kann, wenn sie Microsoft 365 Copilot und/oder Azure OpenAI Service verwenden möchten.



Was sind die wichtigsten Verpflichtungen der DSGVO, die für generative KI-Systeme gelten?

Die Verpflichtungen aus der DSGVO gelten immer dann, wenn ein generatives KI-System personenbezogene Daten verwendet oder anderweitig verarbeitet.

Zu den wichtigsten Verpflichtungen, die Unternehmen bei der Einführung generativer KI-Systeme berücksichtigen sollten, zählen:

- Prüfung, ob Sie Ihre Datenschutzhinweise aktualisieren müssen, um neue Verarbeitungsaktivitäten widerzuspiegeln oder Aktivitäten zu verdeutlichen (Artikel 12 bis 14 DSGVO)
- Sicherstellung, dass Sie über Prozesse verfügen, die es Ihnen ermöglichen, Anträgen zu Betroffenenrechten nachzukommen (Artikel 15 bis 21 DSGVO)
- Sicherstellung, dass jede Vereinbarung, die Sie mit einem Datenverarbeiter getroffen haben, Artikel 28 DSGVO entspricht, auch in Bezug auf Sicherheitsmaßnahmen und internationale Übertragungen
- Prüfung, ob Sie eine Datenschutz-Folgenabschätzung (DSFA) durchführen müssen (Artikel 35 DSGVO)
- Sicherstellung, dass alle Datenübertragungen außerhalb von UK, der EU oder des EWR einem gültigen Übermittlungsmechanismus unterliegen (Artikel 44 bis 50 DSGVO)

In Teil 2 des Leitfadens erfahren Sie mehr darüber, wie Microsoft Kunden bei der Erfüllung dieser Verpflichtungen unterstützt.

Wie interagiert die DSGVO mit dem AI Act?

Der AI Act ist ein neues Gesetz, das derzeit in der EU in Kraft tritt, um KI-Systeme zu regulieren. Sie gilt für Anbieter, Importeure, Vertreiber, Nutzer und andere am KI-Lebenszyklus beteiligte Personen und soll sicherstellen, dass KI-Systeme, die in der EU eingesetzt werden, die Grundrechte, die Sicherheit und die ethischen Grundsätze achten und bestimmte Risiken im Zusammenhang mit den leistungsfähigsten „General Purpose"-KI-Modellen angehen.

Die DSGVO und der AI Act sollen sich ergänzen und nebeneinander wirken und einen regulatorischen Rahmen für KI-Produkte und -Dienste bieten.

Die DSGVO, die die Verarbeitung personenbezogener Daten durch Datenverantwortliche und Datenverarbeiter regelt, konzentriert sich auf den Datenschutz und zielt darauf ab, Einzelpersonen die Kontrolle über ihre personenbezogenen Daten zu geben. Nach dem AI Act wird der größte Teil der regulatorischen Last auf die Anbieter von Hochrisiko-KI-Systemen und „General Purpose"-KI-Modellen (GPAI) fallen.

Obwohl sich die DSGVO und der AI Act in ihrem Geltungsbereich und Zweck unterscheiden, interagieren sie auf verschiedene Weise miteinander. Zum Beispiel:

- Die DSGVO verlangt von den für die Datenverarbeitung Verantwortlichen, unter bestimmten Umständen eine DSFA durchzuführen. Der AI Act bezieht sich auf diese Verpflichtung und verlangt von Nutzern von KI-Systemen mit hohem Risiko, bestimmte obligatorische nutzerbezogene Informationen zu verwenden, um ihren DSFA-Verpflichtungen gemäß der DSGVO nachzukommen.
- Die DSGVO findet Anwendung, wenn personenbezogene Daten verarbeitet werden, um ein KI-System zu trainieren, oder wenn ein KI-System zur Verarbeitung personenbezogener Daten verwendet wird.

Die Verabschiedung der in diesem Dokument dargelegten Maßnahmen zur Einhaltung der DSGVO ist daher eine Ergänzung zum AI Act und den damit verbundenen Verpflichtungen, die nach dieser neuen Gesetzgebung gelten werden.

Bei Microsoft verpflichten wir uns zur Einhaltung des EU AI Act. Unsere langjährigen Bemühungen um die Definition, Weiterentwicklung und Implementierung unseres Microsoft Responsible AI Standards und der internen Governance haben uns dafür eine ideale Ausgangsposition verschafft. Da die endgültigen Anforderungen des EU AI Acts noch detaillierter ausgearbeitet werden, freuen wir uns darauf, gemeinsam mit politischen Entscheidungsverantwortlichen eine praktikable Umsetzung und Anwendung der Regeln sicherzustellen, unsere Compliance zu demonstrieren und mit unseren Kunden und anderen Interessengruppen zusammenzuarbeiten, um die Einhaltung der Vorschriften im gesamten Ecosystem zu unterstützen.

Wie hält Microsoft geltendes Recht ein?

Die KI-Produkte und -Lösungen von Microsoft sind so konzipiert und entwickelt, dass sie den geltenden Datenschutzgesetzen, einschließlich der DSGVO, entsprechen.

Der Ansatz von Microsoft zum Schutz der Privatsphäre in der KI wird durch die Verpflichtung zur Einhaltung bestehender und neuer regulatorischer und rechtlicher Verpflichtungen weltweit untermauert. Wir setzen uns kontinuierlich für eine sinnvolle Regulierung des Datenschutzes und der KI ein und sind überzeugt, dass der beste Weg, um schnelle Fortschritte bei den erforderlichen Leitplanken für KI zu erzielen, darin besteht, sich auf bestehende rechtliche Schutzmaßnahmen, Ansätze und regulatorische Instrumente zu stützen, die heute zum Schutz der Privatsphäre und der Sicherheit in diesen Systemen angewendet werden können.

Gibt Microsoft Kundendaten an OpenAI/ChatGPT weiter?

Nein. Die Kundendaten Ihrer Organisation, einschließlich Prompts (Eingaben) und Vervollständigungen (Ausgaben), Ihre Einbettungen und jegliche Trainingsdaten, die Sie möglicherweise den Microsoft Online Services zur Verfügung stellen, sind für OpenAI nicht verfügbar.

Der Azure OpenAI Service wird vollständig von Microsoft verwaltet. Microsoft hostet die OpenAI-Modelle in der Azure-Umgebung von Microsoft, und Azure OpenAI Service interagiert nicht mit Diensten, die von OpenAI betrieben werden (z. B. ChatGPT oder die OpenAI-API). OpenAI ist kein Unterauftragsverarbeiter von Microsoft.

Erfahren Sie mehr über die zugrundeliegenden OpenAI-Modelle, die Azure OpenAI Service unterstützen.

Kann ich in den generativen KI-Diensten von Microsoft mit vertraulichen Informationen arbeiten?

Ja. Bei der Verwendung von Azure OpenAI oder Microsoft 365 Copilot können Kunden auch sensible Informationen vertrauensvoll übermitteln. Die Foundation-Modelle, auf die über Azure OpenAI Service und Microsoft 365 Copilot zugegriffen wird, verwenden Kundendaten nicht ohne Erlaubnis für das Training. Diese Foundation-Modelle sind „stateless" und speichern keine Daten sowie weder Prompts, die ein Kunde eingibt, noch Vervollständigungen, die das Modell ausgibt. Kunden können sich auch darauf verlassen, dass ihre vertraulichen Informationen nicht an andere Kunden weitergegeben werden.

Wie schützt Microsoft die Sicherheit in diesem neuen Zeitalter der KI?

Die Sicherheit ist entlang des gesamten Entwicklungslebenszyklus aller unserer Enterprise-Services (einschließlich derjenigen, die generative KI-Technologie enthalten) von Grund auf eingebettet, von der ersten Idee bis zur konkreten Auslieferung.

Azure OpenAI Service und Microsoft 365 Copilot werden in der Azure-Infrastruktur gehostet und durch einige der branchenweit umfassendsten Compliance- und Sicherheitsmaßnahmen geschützt. Bei der Entwicklung dieser Dienste wurde die Nutzung der gleichen Sicherheits- und Compliance-Funktionen festgelegt, die in der Hyperscale-Cloud von Microsoft bereits gut etabliert sind. Dazu zählen Zuverlässigkeit, Redundanz, Verfügbarkeit und Skalierbarkeit, die alle standardmäßig in unsere Cloud-Services integriert sind.

Da generative KI-Systeme auch Softwaresysteme sind, gelten alle Elemente unseres Security Development Lifecycle: von der Bedrohungsmodellierung über die statische Analyse, den sicheren Aufbau und Betrieb bis hin zur Verwendung starker Kryptografie, Identitätsstandards und mehr.

Unser Security Development Lifecycle wurde zudem um weitere Schritte ergänzt, um uns auf KI-Bedrohungsvektoren vorzubereiten, einschließlich der Aktualisierung der SDL-Anforderung für die Bedrohungsmodellierung, um KI- und Machine-Learning-spezifische Bedrohungen zu berücksichtigen. Wir unterziehen unsere KI-Produkte einem AI-Red-Teaming, um Schwachstellen zu ermitteln und sicherzustellen, dass wir über geeignete Strategien zur Risikominderung verfügen.

Erfahren Sie in Teil 3 dieses Dokuments mehr über die Sicherheit bei Microsoft 365 Copilot und in Teil 4 dieses Dokuments mehr über die Sicherheit bei Azure OpenAI Service.

Sind Datenübertragungen in Länder außerhalb von UK, der EU oder des EWR nach der DSGVO zulässig?

Ja, personenbezogene Daten können in Länder außerhalb von UK, der EU oder des EWR übermittelt werden, wenn bestimmte Bedingungen erfüllt sind, darunter: (a) Es liegt ein Angemessenheitsbeschluss der Europäischen Kommission oder des britischen Außenministers vor (Artikel 45 DSGVO), oder (b) die Übermittlung unterliegt zusätzlichen Garantien, zu denen die EU-Standardvertragsklauseln und das britische IDTA gehören (Artikel 46 DSGVO).

Bei der Übermittlung personenbezogener Daten durch Microsoft außerhalb von UK, der EU oder des EWR werden gültige Übermittlungsmechanismen gemäß der DSGVO verwendet, einschließlich der Zertifizierung des EU-U.S. Data Privacy Frameworks und gegebenenfalls der EU-Standardvertragsklauseln.

Erfahren Sie in Teil 2 dieses Leitfadens mehr darüber, wie Microsoft bei Datenübertragungen in Drittländer vorgeht.

Wo werden meine Daten gespeichert und verarbeitet?

Ihre Entscheidungen für die Datenresidenz werden berücksichtigt, wenn Sie die generativen KI-Produkte und -Dienste von Microsoft verwenden, die lokale Speicher- und/oder Verarbeitungsfunktionen bieten.

Azure OpenAI Service und Microsoft 365 Copilot verarbeiten und speichern Ihre Daten innerhalb der EU/EFTA für Kunden der EU-Datengrenze (EUDB), wie in den Product Terms und der Dokumentation zur Transparenz der EU-Datengrenze dargelegt.

Müssen Unternehmen ein eigenes Data Protection Addendum (DPA) entwickeln?

Nein, die DSGVO verlangt nicht, dass jeder Datenverantwortliche einen individuellen Datenschutzzusatz mit seinen Datenverarbeitern hat. Das Data Protection Addendum von Microsoft entspricht den Anforderungen von Artikel 28 DSGVO.

Es ist für Hyperscale-Cloud-Anbieter nicht rentabel, unterschiedliche Bedingungen für verschiedene Kunden anzubieten, da es gerade die Einheitlichkeit der Dienste ist, die Cloud-Dienste verwaltbarer, skalierbarer, sicherer und kostengünstiger macht als On-Premises-Lösungen. Darüber hinaus könnte die Einführung unterschiedlicher Sicherheitsmaßnahmen oder -standards für verschiedene Kunden die Sicherheit der Microsoft-Dienste als Ganzes unterminieren. Daher ist es für Microsoft nicht möglich, seine internen Prozesse zu ändern oder individuelle vertragliche Verpflichtungen und/oder Vertragsstrukturen für jeden Kunden zu schaffen.

Weitere Informationen zu den Verpflichtungen von Microsoft zur Datenverarbeitung finden Sie in Teil 2 dieses Leitfadens.

Wie können Kunden ihre Nutzung von generativen KI-Diensten so einrichten, dass sie mit der DSGVO konform sind?

Die DSGVO verlangt von den für die Verarbeitung Verantwortlichen, dass sie Datenschutzfragen in jeder Phase ihrer Verarbeitungstätigkeiten berücksichtigen, von der ersten Konzeption bis zur endgültigen Umsetzung.

Die mit dem Einsatz generativer KI verbundenen Risiken variieren je nach spezifischem Anwendungsfall und der damit verbundenen Art, Sensibilität und Menge der personenbezogenen Daten, die im Zusammenhang mit diesem Anwendungsfall verwendet werden.

Eine Möglichkeit, die Einhaltung der DSGVO nachzuweisen, besteht darin, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, die sich auf bestimmte Anwendungsfälle für generative KI-Lösungen bezieht. Eine DSFA hilft Unternehmen, die Datenschutzrisiken zu identifizieren und zu reduzieren. Eine DSFA ist gesetzlich vorgeschrieben, wenn die Verarbeitungstätigkeit voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Auch wenn sie nicht gesetzlich vorgeschrieben ist, ist eine DSFA eine bewährte Praxis und kann Ihnen helfen, die spezifischen Datenschutzrisiken anzugehen, die mit der Implementierung von generativer KI für einen bestimmten Anwendungsfall verbunden sind.

Weitere Informationen zu DSFAs finden Sie in Teil 2 dieses Leitfadens.

Können Kunden die DSGVO einhalten, wenn sie eine Public Cloud zur Nutzung generativer KI-Dienste verwenden?

Die Public-Cloud-Dienste von Microsoft wurden entwickelt, um sicherzustellen, dass sie von Kunden in Übereinstimmung mit der DSGVO genutzt werden können (und viele Kunden nutzen diese Dienste bereits). Sie können die in diesem Dokument dargelegten und in den Product Terms und dem Data Protection Addendum enthaltenen Informationen verwenden, um eine angemessene risikobasierte Evaluierung der vorgeschlagenen Nutzung von Microsoft 365 Copilot und Azure OpenAI Service vorzunehmen und so die Einhaltung der relevanten DSGVO-Anforderungen nachzuweisen.

Wie können Unternehmen ihren Transparenzpflichten gemäß der DSGVO beim Einsatz von KI-Technologien nachkommen?

Die Artikel 12 bis 14 der DSGVO verpflichten Organisationen, betroffenen Personen bestimmte wichtige Informationen darüber zur Verfügung zu stellen, wie ihre personenbezogenen Daten verwendet werden. Diese Informationen werden häufig in Form von Datenschutzhinweisen zur Verfügung gestellt. Wenn Sie eine neue Technologie (z. B. Microsoft 365 Copilot oder Azure OpenAI Service) bereitstellen und beabsichtigen, diese Technologie auf eine Weise zu verwenden, die nicht in Ihren bestehenden Datenschutzhinweisen abgebildet ist, müssen Sie die entsprechenden Datenschutzhinweise aktualisieren, um die neuen Verarbeitungsaktivitäten widerzuspiegeln.

Die Informationen in diesem Dokument sollen Ihnen helfen zu verstehen, wie Microsoft 365 Copilot und Azure OpenAI Service Daten verwenden, und zu bestimmen, welche Informationen an betroffene Personen weitergegeben werden müssen.

Anhang 3

Weiterführende Ressourcen

Microsoft verfolgt das Ziel, allen Kundinnen und Kunden klare Informationen darüber zur Verfügung zu stellen, wie wir Daten verwenden und übermitteln, und die verschiedenen Optionen aufzuzeigen, die sie bei der Verwaltung ihrer Daten haben. Dieser Anhang enthält zusätzliche Ressourcen, auf die Sie zurückgreifen können, um die in diesem Dokument enthaltenen Informationen zu ergänzen und zu vertiefen.

Responsible AI

- Webseite: Fördern verantwortungsvoller KI-Praktiken
- E-Book: Governing AI: A Blueprint for the Future
- Whitepaper: Microsoft Responsible AI Standard
- Bericht: Responsible AI Transparency Report

Microsoft Customer Commitments

- Blog: AI Assurance Program and AI Customer Commitments
- Blog: Customer Copyright Commitment
- Blog: Protecting the data of our commercial and public sector customers in the AI era
- FAQ: Protecting the Data of our Commercial and Public Sector Customers in the AI Era

Hintergrundinformationen zu generativer KI

- Microsoft Learn-Artikel: Azure OpenAI Service-Modelle
- Microsoft Learn-Artikel: Erstellen effektiver Prompts

Data Protection Addendum und Product Terms

- Data Protection Addendum
- Microsoft Product Terms

Data Residency Commitments

- Microsoft Learn-Artikel: EU-Datengrenze
- Webseite: Dokumentation zur Transparenz der Microsoft EU-Datengrenze
- Microsoft Learn-Artikel: Advanced Data Residency in Microsoft 365
- Microsoft Learn-Artikel: Microsoft 365 Multi-Geo

Datenschutz-Folgenabschätzungen (Data Protection Impact Assessments, DPIA)

- Microsoft Learn-Artikel: DPIA Azure für die DSGVO
- Microsoft Learn-Artikel: Datenschutz-Folgenabschätzung

KI für Unternehmen

- Webseite: Lösungen für künstliche Intelligenz | Microsoft AI
- Blog: AI driven businesses surge ahead of competition
- Webseite: Nutzen und Vorteile von KI für Unternehmen
- Infografik: The business opportunity of AI

Microsoft 365 Copilot

- Webseite: Microsoft 365 Copilot
- Webseite: Copilot Lab
- Webseite: Microsoft 365 Copilot-Dokumentation
- Microsoft Learn-Artikel: Daten, Datenschutz und Sicherheit für Microsoft 365 Copilot
- Microsoft Learn-Artikel: Häufig gestellte Fragen zu Datensicherheit und Datenschutz von Copilot bei Dynamics 365 und Power Platform
- Microsoft Learn-Artikel: Microsoft 365-Isolierungssteuerungen
- Microsoft Learn-Artikel: Verschlüsselung in der Microsoft-Cloud
- Webseite: Microsoft Copilot-Szenarienbibliothek

Azure OpenAI Service

- Dokumentation: Azure OpenAI Service – Schnellstarts, Tutorials, API-Referenzleitfäden
- Microsoft Learn-Artikel: Konfigurieren von Nutzungsrechten für Azure Information Protection (AIP)
- Microsoft Learn-Artikel: Data, privacy and security for Azure OpenAI Service
- Microsoft Learn-Artikel: Prompt-Engineering-Techniken
- Microsoft Learn-Artikel: Verwenden Ihrer eigenen Daten mit dem Azure OpenAI Service – Azure OpenAI On Your Data
- Microsoft Learn-Artikel: Überlegungen zur Optimierung (Feinabstimmung) mit Azure OpenAI Service
- Microsoft Learn-Artikel: Inhaltsfilterung
- Microsoft Learn-Artikel: Missbrauchsüberwachung
- Microsoft Learn-Artikel: Unternehmenssicherheit und -governance für Azure Machine Learning