# DSGVO UND GENERATIVE KI
# EIN LEITFADEN FÜR KUNDEN

MAI 2024

Übersetzung aus dem Englischen Microsoft Paper „GDPR & Generative AI - A Guide for Customers“, May 2024

# Kontakt

**Rudolf Palkowitz**
Manager | Microsoft Competence Center
rudolf.palkowitz@msg-plaut.com
+43 664 627 68 22

**msg Plaut Austria GmbH**
Modecenterstraße 17/4/6 , 1110 Wien
msg-plaut.at

## msg Plaut

Die msg Plaut Gruppe ist einer der führenden IT-Dienstleister in Österreich sowie Südost- und Ost-Europa. Mit Sitz in Wien und rund 750 Mitarbeitenden zeichnet sich das Unternehmen besonders durch seine Eigentümerführung sowie einem Beratungs- und Entwicklungsansatz nach den Prinzipien des Digitalen Humanismus, der die Menschen ins Zentrum aller IT-Projekte stellt, aus. Das macht msg Plaut zum Pionier in der Umsetzung ethischer und humanistischer Werte in der digitalen Welt.

In Österreich beschäftigt die msg Plaut Gruppe 200 hochqualifizierte Fachkräfte an drei Standorten und betreut dabei Kunden aus unterschiedlichen Wirtschaftsbereichen, darunter Automotive, Banking & Insurance, Logistik, die produzierende Industrie oder der öffentliche Dienst. Mit einer breiten Palette an eigenentwickelten und Standardprodukten bietet das Unternehmen intelligente IT- und Branchenlösungen, die betriebswirtschaftliche und strategische Beratung mit zukunftsorientierten, nachhaltig wertschöpfenden IT-Lösungen verbinden.

Insbesondere in SAP- und Microsoft-Umgebungen hat sich msg Plaut einen Namen als echter Lösungsexperte in der Branche erarbeitet. Ob Innovationsmanagement oder Safety & Security, ob klassisches Projektmanagement oder individuelle Software-Entwicklung, ob Requirements Engineering, Test- und Quality-Management, Application Management oder Cloud Transformation, digitale Plattformen und Business Intelligence – als Teil der unabhängigen, internationalen msg Gruppe mit 10.000 Spezialisten in 35 Ländern ist msg Plaut ein bedeutender Partner für nationale und internationale Unternehmen, die in der rasant fortschreitenden digitalen Welt auch in ethischer Hinsicht erfolgreich bestehen wollen.

**Mehr Informationen unter msg-plaut.at**

# Inhalt

# Zusammenfassung

- Die Use Cases für generative KI bieten eine spannende Möglichkeit, die Qualität der Dienstleistungen und die betriebliche Effizienz zu verbessern. Microsoft möchte seine Kunden in die Lage versetzen, das volle Potenzial neuer Technologien wie der generativen Künstlichen Intelligenz auszuschöpfen und gleichzeitig ihre Verpflichtungen im Rahmen der Datenschutzgrundverordnung (DSGVO) einzuhalten.
- Microsoft setzt sich dafür ein, dass seine KI-Systeme verantwortungsvoll und auf eine Weise entwickelt werden, dass sie das Vertrauen der Menschen verdient. Microsoft verfolgt diese Verpflichtung anhand von sechs Schlüsselprinzipien, die sich eng an die in Artikel 5 der DSGVO festgelegten Grundprinzipien anlehnen.
- Wenn es um die Einhaltung der DSGVO im Zusammenhang mit der Nutzung generativer KI-Dienste geht, gelten die Grundprinzipien der DSGVO genauso wie bei der Verarbeitung personenbezogener Daten in jedem anderen Kontext (z. B. bei der Nutzung von Cloud-Diensten). KI-Technologie mag zwar neu sein, aber die Grundsätze und dementsprechend auch die Prozesse für Risikobewertungen und Einhaltung der DSGVO bleiben dieselben. Unternehmen können daher sicher sein, dass Microsoft seine KI-Dienste auf die gleiche Weise angeht wie andere Cloud-Dienste auch.
- Die bestehenden Datenschutzverpflichtungen von Microsoft, einschließlich derjenigen, die im Microsoft Data Protection Addendum enthalten sind, gelten auch für Microsofts kommerzielle KI-Produkte. Microsoft-Kunden[1] können sich darauf verlassen, dass jene Datenschutzverpflichtungen, auf die sie sich bei der Nutzung der Cloud-Produkte für Unternehmen schon lange verlassen, auch für Copilot für Microsoft 365 und den Azure OpenAI Service gelten. Kunden können daher sicher sein, dass ihre wertvollen Daten durch branchenführende Data Governance und Datenschutzpraktiken in der vertrauenswürdigsten Cloud auf dem Markt geschützt sind.
- Im Rahmen der DSGVO gibt es eine Reihe wichtiger Verpflichtungen, die Unternehmen bei der Nutzung generativer KI-Dienste berücksichtigen müssen. In diesem Paper hat Microsoft Details zu diesen Verpflichtungen und den damit verbundenen Support und Ressourcen aufgenommen, auch hinsichtlich internationale Übertragung von personenbezogener Daten, Transparenz, Rechte der betroffenen Personen, Verpflichtungen des Verarbeiters, technische und organisatorische Sicherheitsmaßnahmen und Data Privacy Impact Assessments (DPIA).
- Die Daten der Kunden gehören den Kunden. Microsoft erhebt keinen Anspruch auf das Eigentum an Kundenprompts oder Ausgabeinhalten, die von Microsofts generativen KI-Lösungen erstellt wurden. Darüber hinaus werden keine Kundendaten (einschließlich Prompts oder Ausgabeinhalte) ohne die Zustimmung des Kunden zum Trainieren von Foundation-Modellen verwendet.
- Während sich die regulatorische Landschaft weiterentwickelt und Microsoft neue Arten von KI-Lösungen anbietet, wird Microsoft weiterhin branchenführende Tools, Ressourcen und Support anbieten, um Engagement für die Erfüllung von Kundenbedürfnisses und -Anforderungen bei ihrer KI-Reise zu demonstrieren.

[1] Dieser Leitfaden gilt für die Nutzung der kostenpflichtigen Unternehmensdienste für Copilot für Microsoft 365 und den Azure OpenAI Service. Alle Verweise in diesem Leitfaden auf „Kunden“ beziehen sich auf private Körperschaften und / oder Unternehmen. Der Inhalt dieses Papers gilt nicht für Verbraucher oder Einzelpersonen, die Microsoft-Lösungen in ihrer persönlichen Eigenschaft nutzen. Microsoft hat auch eine Version dieses Whitepapers für Kunden des öffentlichen Sektors erstellt, die unter dem folgenden Link abgerufen werden kann: DSGVO und generative KI - Ein Leitfaden für den öffentlichen Sektor.

# Einführung

In der sich schnell entwickelnden Geschäftslandschaft von heute stehen Unternehmen zunehmend unter Druck, innovativ zu sein, höhere Effizienz zu erreichen und das Kundenerlebnis zu verbessern. Dies führt dazu, dass Unternehmen nach Wettbewerbsvorteilen suchen, indem sie das Potenzial generativer KI-Lösungen nutzen. Durch die Automatisierung von Routineaufgaben, die Bereitstellung tiefgreifender analytischer Erkenntnisse und Entscheidungen in Echtzeit können generative KI-Lösungen Unternehmen dabei helfen, auf Marktdynamiken zu reagieren.

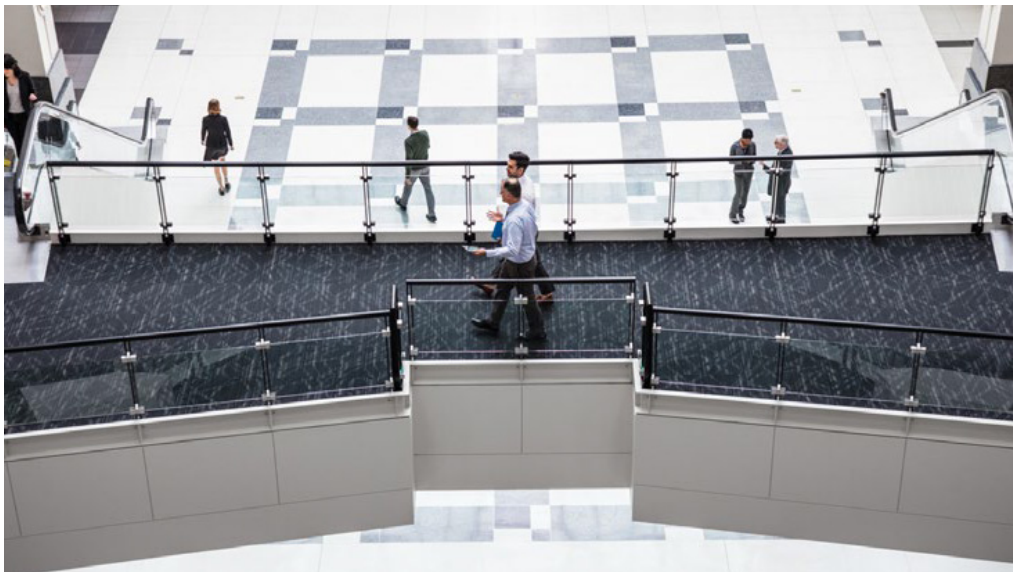
Es besteht kein Zweifel, dass KI die Zukunft der Arbeitsweise von Unternehmen prägen wird. Der geschäftliche Nutzen von KI liegt auf der Hand: Sie hilft Unternehmen, effizienter zu arbeiten, bessere Leistungen zu erbringen, mehr zu erreichen und die erforderlichen Erkenntnisse zu gewinnen, um bessere Entscheidungen zu treffen. Darüber hinaus hat sich gezeigt, dass sich Investitionen in KI-Lösungen positiv auf das Endergebnis eines Unternehmens auswirken.[2]

Generative KI-Lösungen können in Unternehmen auf jeder Ebene optimieren und neue wertvolle Möglichkeiten aufdecken. Um diese Wirkung mit KI-Innovationen zu erzielen, muss sichergestellt werden, dass Unternehmen effiziente und vertrauenswürdige KI-Lösungen auswählen und dass diese auf verantwortungsvolle und sichere Weise implementieren, wobei die Notwendigkeit des Schutzes personenbezogener Daten berücksichtigt werden muss.

Microsoft möchte seine Kunden in die Lage versetzen, das volle Potenzial neuer Technologien, wie der generativen KI, zu nutzen und gleichzeitig ihre Verpflichtungen gemäß der Datenschutzgrundverordnung (DSGVO) zu erfüllen, um den Schutz und die Sicherheit von Daten zu gewährleisten.

Der Schutz von Kundendaten hat eine lange Tradition. Microsofts Ansatz für verantwortungsbewusste KI basiert auf der Wahlung der Privatsphäre, und sie setzen sich weiterhin für die Einhaltung der Kernwerte Datenschutz, Sicherheit und Schutz in allen generativen KI-Produkten und -Lösungen von Microsoft ein. Mit der zunehmenden Nutzung von KI-Lösungen können Kunden darauf vertrauen, dass ihre Daten durch branchenführende Data-Governance- und Datenschutzpraktiken in einer der vertrauenswürdigsten Clouds geschützt werden. Kunden können sich darauf verlassen, dass die Datenschutzverpflichtungen, auf die sie sich bei der Nutzung der Microsoft Cloud-Produkte für Unternehmen seit langem verlassen, auch für Microsofts generative KI-Lösungen für Unternehmen gelten, die durch das Microsoft Data Protection Addendum unterstützt werden, einschließlich Copilot für Microsoft 365 und Azure OpenAI Service.

Als Branchen- und Vordenker auf dem Gebiet der KI hat Microsoft dieses Paper entwickelt, um spezifische Bedenken in Bezug auf die DSGVO-konforme Nutzung von Copilot für Microsoft 365 und den Azure OpenAI Service für Kunden in Europa anzusprechen und um zu zeigen, wie Microsofts KI-Lösungen DSGVO-konform eingesetzt werden können.



[2] Für jeden 1 Dollar, den ein Unternehmen in KI investiert, erzielt es eine durchschnittliche Rendite von 3,50 Dollar und es dauert durchschnittlich 14 Monate, bis sich die KI-Investitionen amortisiert haben. Quelle: IDC, Die Geschäftsmöglichkeit von KI, November 2023

# Aufbau dieses Microsoft-Papers

## Teil 1

untersucht die Bedeutung von verantwortungsbewusster KI, die sechs Schlüsselprinzipien und den Ansatz für verantwortungsbewusste KI, die Microsoft bei der Entwicklung von KI-Produkten leiten, und zeigt die Tools und Ressourcen auf, die Microsoft zur Unterstützung Ihrer KI-Implementierung anbietet.

## Teil 2

setzt den Fokus auf Struktur und Anforderungen der DSGVO und darauf, wie Microsoft seine Kunden dabei unterstützen kann, KI-Lösungen zu nutzen und gleichzeitig Compliance-Verpflichtungen gemäß der DSGVO zu erfüllen.

## Teil 3 und 4

sind einer eingehenden Untersuchung von Copilot für Microsoft 365 und dem Azure OpenAI Service gewidmet, und wie diese Dienste in Übereinstimmung mit der DSGVO genutzt werden können.

## Teil 5

schließt das Paper mit einem Rückblick auf die gewonnenen Erkenntnisse und die künftige Entwicklung von KI und Datenschutzregulierung.

## Anhang 1

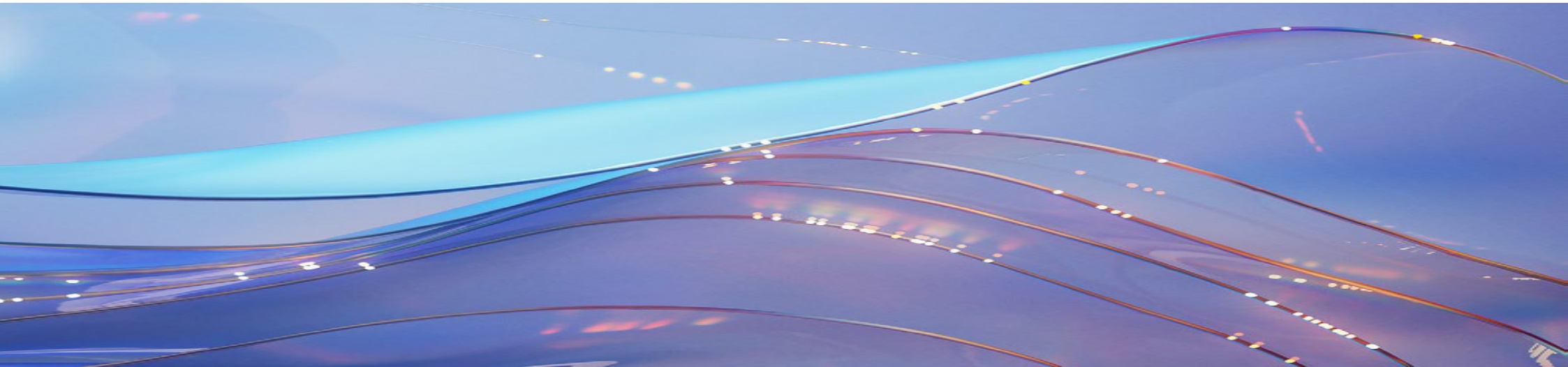
zeigt einige der aufregenden Möglichkeiten, die generative KI für Unternehmen in verschiedenen Branchen bietet.

## Anhang 2

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

## Anhang 3

enthält Links zu weiteren Ressourcen, auf die Kunden zurückgreifen können, um ihr Wissen zu den in diesem Dokument enthaltenen Informationen zu ergänzen und zu erweitern.



# Teil 1: Verantwortungsvolle Nutzung von KI: Microsofts KI-Reise und Nutzung von Tools und Ressourcen

## Verantwortungsvolle KI

KI hat das Potenzial, Unternehmen zu verändern, von der Rationalisierung von Mitarbeitendenaufgaben bis hin zur Beschleunigung von Dienstleistungen und Produkten. Das wachsende Interesse an generativer KI ist offensichtlich. Mit dieser „großen Macht kommt jedoch auch große Verantwortung“, und deshalb ist es wichtig, dass KI verantwortungsvoll entwickelt und eingesetzt wird. Microsoft hat mit der Entwicklung umfassender KI-Verantwortungsrichtlinien und -Werkzeuge, die auf ihrer langjähriger Arbeit beruhen, eine prinzipielle Rolle in diesem Bereich übernommen.

Der gewissenhafte Einsatz von KI ist ein Thema, mit dem sich Unternehmen auf der ganzen Welt in den letzten Jahren aktiv auseinandergesetzt haben. Durch Diskussionen, Entwicklungen von Ansätzen und Strategien und deren Umsetzung in ihren Betrieben ist die Nutzung von KI zur Bereitstellung verantwortungsvoller, produktiverer, effizienterer und innovativerer Produkte und / oder Dienstleistungen auf dem Vormarsch.

> Mehr Informationen über Governing AI: A Blueprint for the Future

Microsoft setzt sich dafür ein, dass KI-Systeme verantwortungsvoll und auf eine Weise entwickelt werden, die das Vertrauen der Menschen verdient. Das Engagement beruht auf sechs Grundsätzen, die sich eng an die in Artikel 5 der DSGVO festgelegten Grundprinzipien anlehnen:

+ **Fairness:** KI-Systeme sollten so konzipiert sein, dass sie alle Personen fair und ohne Vorurteile oder Diskriminierung behandeln.
+ **Verlässlichkeit und Sicherheit:** KI-Systeme sollten zuverlässig und sicher sein, mit eingebauten Mechanismen zur Fehlervermeidung und Schadensminimierung.
+ **Rechenschaftspflicht:** Die Erfinder von KI-Tools und die Entwickler, die sie einsetzen, sollten für ihre Systeme verantwortlich sein.
+ **Privatsphäre und Sicherheit:** KI-Systeme sollten die Privatsphäre des Einzelnen und die Datensicherheit respektieren.
+ **Inklusion:** KI-Systeme sollten so konzipiert sein, dass sie für jeden zugänglich und nutzbar sind, auch für Menschen mit Behinderungen.
+ **Transparenz:** KI-Systeme sollten transparent und erklärbar sein, mit einer klaren Dokumentation ihrer Funktionen und Entscheidungsprozesse.

Diese Grundsätze können von Kunden genutzt werden, um KI-Systeme und -Prozesse zu bewerten, die im Zusammenhang mit der DSGVO im Einsatz sind oder in Erwägung gezogen werden, wie in Teil 2 nachstehend beschrieben. Innerhalb von Microsoft wurde das Office of Responsible AI eingerichtet, das die KI-Governance-Richtlinien für das gesamte Unternehmen festlegt, das Senior Leadership-Team in KI-Fragen berät und es den Engineering- und Compliance-Teams im gesamten Unternehmen ermöglicht, nach den Grundsätzen der verantwortungsvollen KI zu arbeiten, während Microsoft gleichzeitig sicherstellt, dass das Unternehmen seine ethische Haltung kontinuierlich überprüft und verbessert, wenn neue Möglichkeiten und Herausforderungen entstehen.

> Mehr Informationen über die Grundsätze und den Ansatz von Microsoft für verantwortungsvolle KI

Im Mai 2024 hat Microsoft seinen ersten Responsible AI Transparency Report veröffentlicht, der auf dem Microsoft-internen Responsible AI Standard aufbaut. Dieser Bericht gibt Einblick in die Art und Weise, wie Microsoft Anwendungen entwickelt, die generative KI nutzen, wie Prompt-Entscheidungen trifft und den Einsatz dieser Anwendungen überwacht, und auch wie Microsoft seine Kunden bei der Entwicklung ihrer eigenen generativen Anwendungen unterstützt und sie als verantwortungsbewusste KI-Community lernt, sich weiterzuentwickeln und zu wachsen.

Unternehmen sollten verantwortungsvolle KI-Strategien entwickeln und sich an diese halten. Diese Strategien sollten Prinzipien,

Praktiken, Tools und Governance beinhalten, die es den Mitarbeitenden in der gesamten Unternehmen ermöglicht, den Einsatz von KI zu bewerten, anzunehmen und zu verwalten.

Wenn potenzielle Risiken verstanden und sorgfältig gemanagt werden, können Unternehmen das Versprechen der KI realisieren. Vorausschauende Führungskräfte stellen sicher, dass ihr Engagement für verantwortungsvolle KI kein nachträglicher Gedanke ist, sondern in die Innovationspipeline ihres Unternehmens integriert ist. Auf diese Weise können Unternehmen die Leistung von KI nutzen, um ihre Produkte und / oder Dienstleistungen zu verbessern und profitablere Ergebnisse zu erzielen.

In Anhang 1 finden sich einige spannende Beispiele für den Einsatz generativer KI.

## Tools, Verpflichtungen und Ressourcen zur Unterstützung der KI-Implementierung

Um seinen Kunden zu unterstützen und ihnen die regelkonforme Nutzung von KI zu ermöglichen, bietet Microsoft eine Reihe von Lösungen, Werkzeugen und Ressourcen an, die bei ihrer KI-Implementierung unterstützen. Von einer umfassenden Transparenzdokumentation bis hin zu einer Reihe von Tools für Data Governance, Risiko- und Compliance-Bewertung. Spezielle Programme wie Microsofts branchenführendes AI Assurance Program und AI Customer Commitments erweitern den Support, die Microsoft-Kunden bei der Erfüllung ihrer Anforderungen bietet.

Das Microsoft AI Assurance Program hilft Kunden sicherzustellen, dass KI-Anwendungen, die sie auf Microsoft Plattformen einsetzen, die rechtlichen und regulatorischen Anforderungen für verantwortungsvolle KI erfüllen. Das Programm umfasst Unterstützung bei der Einbindung von Regulierungsbehörden, bei der Implementierung von Risikorahmen und bei der Einrichtung eines Kundenbeirats.

Seit Jahrzehnten verteidigt Microsoft seine Kunden gegen Ansprüche auf geistiges Eigentum im Zusammenhang mit Microsoft Produkten. Aufbauend auf den früheren Microsoft-KI-Kundenverpflichtungen kündigte Microsoft seine Kundenverpflichtung zum Urheberrecht an, die Unterstützung bei der Entschädigung für geistiges Eigentum sowohl auf Copilot für Microsoft 365 als auch auf Azure OpenAI Services ausweitet. Wenn nun ein Dritter einen Kunden wegen Urheberrechtsverletzungen verklagt, weil er Copilot für Microsoft 365 oder den Azure OpenAI Service verwendet, oder wegen der von ihnen erzeugten Ausgabe, wird Microsoft den Kunden verteidigen und den Betrag aller nachteiligen Urteile oder Vergleiche bezahlen, die sich aus dem Rechtsstreit ergeben, solange der Kunde die Schutzmechanismen und Inhaltsfilter verwendet hat, die Microsoft in seine Produkte eingebaut habt.

Microsoft hat mit Microsoft Purview auch eine Reihe von Lösungen entwickelt, die Kunden bei der Datenverwaltung unterstützen. Weitere Einzelheiten dazu, wie Microsoft Purview die Einhaltung der DSGVO unterstützen kann, finden sich in Teil 2.

# Teil 2: Der DSGVO-Compliance-Rahmen im Kontext der KI

## Was ist die DSGVO und für wen gilt sie?

Die DSGVO[3] setzt weltweit einen wichtigen Maßstab für Datenschutzrechte, Informationssicherheit und Compliance. Bei Microsoft schätzt man die Privatsphäre als ein Grundrecht, und denkt, dass die DSGVO eine wichtige Rolle beim Schutz und der Ermöglichung der Datenschutzrechte des Einzelnen spielt.

Microsoft hat sich selbst zur Einhaltung der DSGVO verpflichtet und stellt eine Reihe von Produkten, Funktionen, Dokumentationen und Ressourcen zur Verfügung, um seine Kunden bei der Erfüllung ihrer Verpflichtungen im Rahmen der DSGVO zu unterstützen.

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

Jede Unternehmen, die personenbezogene Daten von betroffenen Personen mit Wohnsitz in Europa verarbeitet, unterliegt der DSGVO. Auch nationale Gesetze enthalten Datenschutzvorschriften und -Richtlinien. Diese werden im Allgemeinen so angepasst, dass sie die Anforderungen der DSGVO erfüllen und / oder übertreffen.

## Nutzung etablierter Grundsätze zur Einhaltung der rechtlichen Rahmenbedingungen bei der Nutzung von KI-Lösungen

Wenn Microsoft über die DSGVO im Zusammenhang mit dem Einsatz generativer KI und der Nutzung der durch diese Technologie gebotenen Möglichkeiten spricht, ist der Ausgangspunkt, dass die Grundprinzipien der DSGVO nach wie vor in derselben Weise gelten wie für die Verarbeitung personenbezogener Daten in jedem anderen Kontext, auch bei Cloud-Nutzung. Die KI-Technologie mag zwar neu sein, aber die Grundsätze und dementsprechend auch die Prozesse für die Risikobewertung und die Einhaltung der DSGVO bleiben dieselben.

Es ist auch hilfreich zu erkennen, dass die DSGVO technologieunabhängig verfasst wurde und Unternehmen daher nicht daran hindert, Möglichkeiten zur Nutzung generativer KI zu ergreifen.

Daher ist die Anwendung etablierter DSGVO-Bewertungsprozesse eine großartige Möglichkeit für Unternehmen, das revolutionäre KI-Potenzial zu nutzen und großartige Ergebnisse zu erzielen, während gleichzeitig die Privatsphäre und das Wohlergehen der Menschen geschützt werden. Microsoft arbeitet seit langem mit seinen Kunden zusammen und unterstützt sie bei der Umsetzung ihrer Prioritäten im Bereich der digitalen Transformation, wobei die Anforderungen der DSGVO eingehalten werden, auch in Bezug auf den Übergang von On-Premises zu Cloud Computing. Kunden können sich den generativen KI-Lösungen von Microsoft nähern, indem sie den Ansatz nutzen, den sie bei der Verwendung der Cloud-Dienste gewählt haben.

Cloud Computing ist für den Zugriff auf die potenziell bahnbrechende KI-Technologie unerlässlich, und die Hyper-Scale-Cloud ist daher Grundlage für den Einsatz von KI. Die unternehmensgerechten Schutzmaßnahmen von Azure, die Teil von Copilot für Microsoft 365 und des Azure OpenAI Service sind, bieten eine solide Grundlage, auf der Kunden ihre Datenschutz-, Sicherheits- und Compliance-Systeme aufbauen können, um KI vertrauensvoll zu skalieren und gleichzeitig Risiken zu managen und die Einhaltung der DSGVO zu gewährleisten.

[3] Für dieses Dokument gelten alle Verweise auf die EU-DSGVO auch für die britische DSGVO.

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

Im Rahmen der DSGVO gibt es zwei wichtige Parteien, die jeweils eigene Verantwortungen für die Einhaltung der Vorschriften haben:

+ Der **für die Datenverarbeitung Verantwortliche** entscheidet, warum und wie personenbezogene Daten verarbeitet werden, und ist die Stelle, die in erster Linie den durch die DSGVO auferlegten Verpflichtungen unterliegt. Viele dieser Verpflichtungen gelten ab dem Zeitpunkt, zu dem diese Stelle beginnt, personenbezogene Daten über Personen zu sammeln.
+ Im Gegensatz dazu ist der **Datenverarbeiter** nach der DSGVO im Wesentlichen ein Unterauftragnehmer des für die Datenverarbeitung Verantwortlichen, der personenbezogene Daten im Namen und auf Anweisung des für die Datenverarbeitung Verantwortlichen verarbeitet.

Unternehmen können im Rahmen der DSGVO als für die Datenverarbeitung Verantwortliche UND als Datenverarbeiter auftreten. Bei der Nutzung der generativen KI-Dienste von Microsoft wird in den Produktbedingungen von Microsoft angegeben, ob Microsoft einen Onlinedienst als Datenverarbeiter oder als für die Verarbeitung Verantwortlicher bereitstellt. Die meisten Onlinedienste, einschließlich der generativen KI-Dienste, werden von Microsoft als Datenverarbeiter bereitgestellt und unterliegen dem Datenschutzzusatz (DPA). Weitere Einzelheiten zu bestimmten Produkten und Diensten finden sich in den Microsoft-Produktbedingungen.

## 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.

Microsoft-Kunden müssen festlegen, wie diese Tools und Dienste genutzt werden und welche personenbezogenen Daten verarbeitet werden, damit Sie sicherstellen können, dass Sie diese Tools in einer konformen Weise genutzt werden.

Um Sie dabei zu unterstützen, hat Microsoft seine generativen KI-Tools und -Dienste mit Blick auf den Schutz der Privatsphäre und den Datenschutz entwickelt und stellt den Kunden Informationen, Funktionen und vertragliche Verpflichtungen zur Verfügung, um Sie bei der Einhaltung Ihrer Verpflichtungen zur Einhaltung und Rechenschaftspflicht gemäß der DSGVO zu unterstützen. Die folgenden Abschnitte in diesem Teil 2 gehen näher darauf ein und stellen Ihnen Informationen zur Verfügung, die Sie bei der Bewertung der Nutzung der generativen KI- Tools und -Dienste von Microsoft in Übereinstimmung mit der DSGVO unterstützen.

## Wie unterstützt Microsoft seine Kunden bei der Einhaltung der DSGVO-Verpflichtungen?

Da immer mehr Unternehmen versuchen, generative KI zu nutzen, sehen viele Microsoft nicht nur als Dienstleister, sondern auch als vertrauenswürdigen Partner auf dem Weg zur Erfüllung ihrer Compliance-Verpflichtungen im Rahmen der DSGVO.

Der erste Schritt auf dem Weg zur Compliance besteht darin, zu verstehen, wie die generativen KI-Dienste von Microsoft funktionieren und wie sie personenbezogene Daten verarbeiten. Microsofts umfassende Transparenzdokumentation und Informationen helfen zu verstehen, wie Microsoft KI-Tools funktionieren und welche Entscheidungen Kunden treffen können, um die Leistung und das Verhalten des Systems zu beeinflussen.

In Teil 3 und Teil 4 dieses Papers finden sich spezifische Informationen und Links zu weiteren Ressourcen, die genutzt werden können, um das Verständnis für diese Produkte und Dienstleistungen zu verbessern.

Teil 3 liefert mehr Informationen zu Copilot für Microsoft 365, Teil 4 zu Azure OpenAI Services.

Dieses Wissen bildet die Grundlage für die Einhaltung einer Reihe von Schlüsselverpflichtungen im Rahmen der DSGVO.

Microsoft wird diese Schlüsselverpflichtungen und die damit verbundene Unterstützung, die Microsoft seinen Kunden anbietet, später in diesem Teil 2 untersuchen, aber zunächst Details zu den Datenschutzverpflichtungen, die Microsoft seinen Kunden in der KI-Ära anbietet.

## Schutz der Kundendaten -

## Microsofts Datenschutzverpflichtungen in der KI-Ära

Die bestehenden Datenschutzverpflichtungen von Microsoft erstrecken sich auch auf die kommerziellen KI-Produkte, wie in einem Blogbeitrag von Microsofts Chief Privacy Officer Julie Brill erläutert wird. Microsoft-Kunden können sich darauf verlassen, dass die Datenschutzverpflichtungen, auf die sie sich seit langem bei der Nutzung von Microsoft Enterprise Cloud-Produkten verlassen, auch für die generativen KI-Lösungen für Unternehmen gelten, die von Microsofts Datenschutzzusatz (DPA) (Data Protection Addendum - DPA) unterstützt werden, einschließlich Copilot für Microsoft 365 und Azure OpenAI Service.

Die folgenden sieben Verpflichtungen gelten für „Kundendaten“, die in den Produktbedingungen von Microsoft als alle Daten, einschließlich aller Text-, Ton-, Video- oder Bilddateien und Software, definiert sind, die Microsoft von oder im Namen von Micosoft-Kunden durch die Nutzung eines Online-Dienstes zur Verfügung gestellt werden.

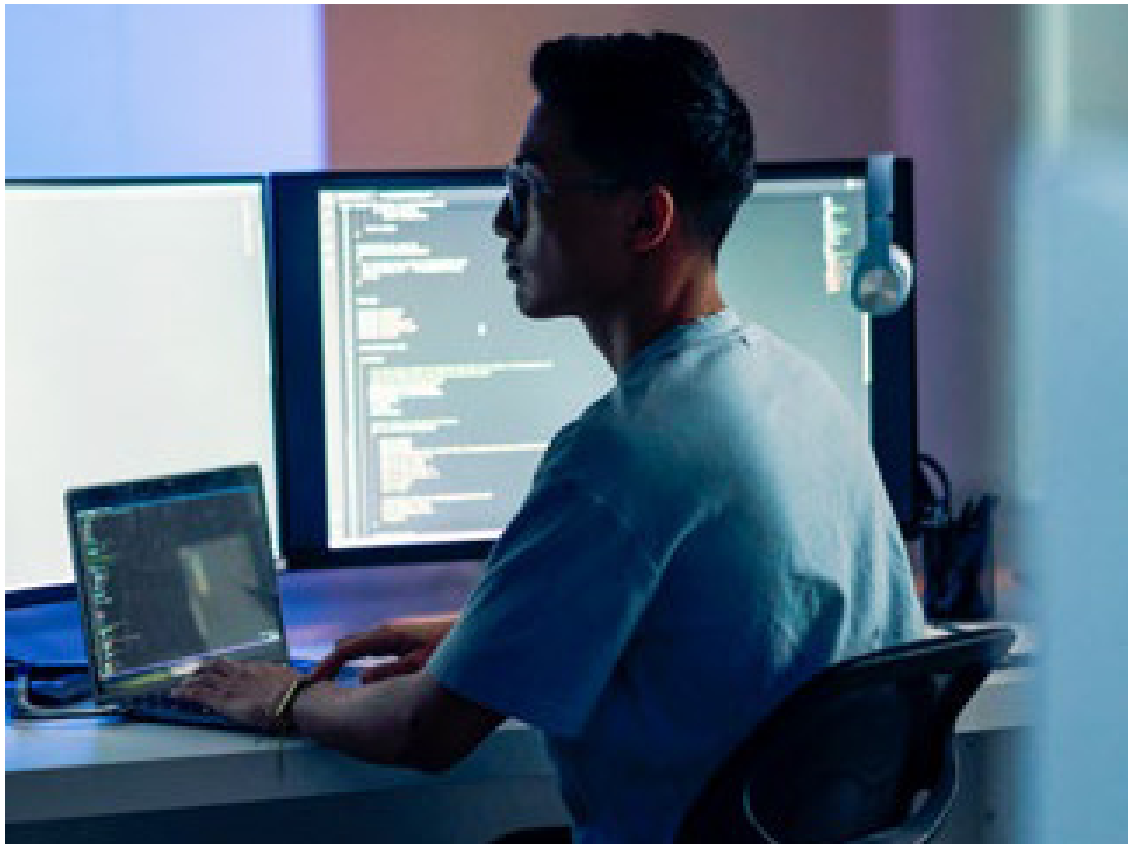
Alle Eingaben (einschließlich Prompts)[4] und Ausgabeinhalte[5] sind Kundendaten. Gemäß dem Datenschutzzusatz (DPA) von Microsoft behält der Kunde „alle Rechte, Titel und Interessen an und in den Kundendaten“.

## Die Daten der Unternehmen werden vertraulich behandelt

Daten bleiben bei der Nutzung von Copilot für Microsoft 365 und Azure OpenAI Service privat und unterliegen den geltenden Datenschutz- und Vertragsverpflichtungen, einschließlich der Verpflichtungen, die in Microsofts Datenschutzzusatz (DPA) und Microsofts Produktbedingungen eingehen.

## Kunden haben die Kontrolle über die Daten Ihres Unternehmens

Daten werden nicht auf unbekannte Weise oder ohne Zustimmung verwendet. Kunden können sich dafür entscheiden, die Nutzung von Copilot für Microsoft 365 oder Azure OpenAI Service anzupassen, indem Daten zur Feinabstimmung von Modellen für die eigene Verwendung im Unternehmen verwendet werden. Wenn die Daten des Unternehmens für die Feinabstimmung verwendet werden, sind alle fein abgestimmten KI-Lösungen, die mit den Daten des Unternehmens erstellt wurden, nur für dieses verfügbar.



4 „Eingaben“ bezeichnet alle Kundendaten, die der Kunde zur Verwendung durch eine generative Technologie der künstlichen Intelligenz bereitstellt, bestimmt, auswählt oder eingibt, um eine Ausgabe zu erzeugen oder anzupassen, einschließlich aller Prompts.

5 „Ausgabeinhalt“ bezeichnet alle Daten, Texte, Töne, Videos, Bilder, Codes oder sonstigen Inhalte, die von einem Modell als Reaktion auf eine Eingabe erzeugt werden.

## Zugriffskontrollen und Unternehmensrichtlinien werden beibehalten

Zum Schutz der Privatsphäre bei der Verwendung von Unternehmensprodukten mit generativen KI-Funktionen gelten weiterhin die bestehenden Berechtigungen und Zugriffskontrollen, um sicherzustellen, dass die Daten des Unternehmens nur denjenigen Benutzern angezeigt werden, denen entsprechende Berechtigungen erteilt wurden.

## Daten von Unternehmen werden nicht weitergegeben

Microsoft gibt Daten nicht ohne Zustimmung an Dritte weiter. Daten, einschließlich der Daten, die durch die Nutzung von Copilot für Microsoft 365 oder Azure OpenAI Service durch Unternehmen generiert werden - wie z. B. Prompts und Antworten - werden privat gehalten und nicht an Dritte weitergegeben.

## Der Datenschutz und die Datensicherheit von Unternehmen sind by design geschützt

Sicherheit und Datenschutz werden in allen Phasen der Entwicklung und Implementierung von Copilot für Microsoft 365 und Azure OpenAI Service berücksichtigt. Wie bei allen Produkten bietet Microsoft eine starke Datenschutz- und Sicherheitsbasis und stellt zusätzliche Schutzmaßnahmen zur Verfügung, die aktiviert werden können. Da sich die Bedrohungen von außen weiterentwickeln, wird Microsoft seine Lösungen und Angebote weiter verbessern, um erstklassigen Datenschutz und Sicherheit in Copilot für Microsoft 365 und Azure OpenAI Service zu gewährleisten, und wird seinen Ansatz weiterhin transparent machen.

## Die Daten eines Unternehmens werden nicht zum Trainieren von Foundation-Modellen verwendet

Die generativen KI-Lösungen von Microsoft, einschließlich Copilot für Microsoft 365 und Azure OpenAI Service- Funktionen, verwenden keine Kundendaten zum Trainieren von Basismodellen ohne Zustimmung. Kundendaten sind niemals für OpenAI verfügbar oder werden zur Verbesserung von OpenAI-Modellen verwendet.

## Microsoft Produkte und Lösungen entsprechen den weltweiten Datenschutzbestimmungen

Die KI-Produkte und -Lösungen von Microsoft entsprechen den heutigen globalen Datenschutz- und Datensicherheitsvorschriften. Während Microsoft die Zukunft der KI gemeinsam gestaltet, einschließlich der Umsetzung des EU-KI-Gesetzes und anderer globaler Gesetze, können Unternehmen sicher sein, dass Microsoft in Bezug auf Datenschutz-, Sicherheits- und Schutzpraktiken transparent ist. Microsoft hält sich an globale Gesetze, die KI regeln, und untermauern Versprechen mit klaren vertraglichen Verpflichtungen.

Weitere Einzelheiten darüber, wie die Datenschutzverpflichtungen von Microsoft für Azure OpenAI und Copilot für Microsoft 365 gelten, finden sich hier und in den FAQ: Schutz der Daten der Kunden aus dem gewerblichen und öffentlichen Sektor im Zeitalter der KI.

## Die wichtigsten Pflichten nach der DSGVO im Zusammenhang mit generativen KI-Diensten

Im Rahmen der DSGVO gibt es eine Reihe von Verpflichtungen, die Unternehmen bei der Beschaffung von generativen KI- Diensten berücksichtigen müssen. Dieser Abschnitt befasst sich mit einigen der wichtigsten Verpflichtungen und der damit verbundenen Unterstützung und Ressourcen, die Microsoft Unternehmen anbieten kann, um sie bei der Einhaltung zu unterstützen.

## Artikel 12 bis 14 der DSGVO (Transparenz)

Nach den Artikeln 12 bis 14 der DSGVO müssen die für die Verarbeitung Verantwortlichen den betroffenen Personen bestimmte Schlüsselinformationen über die Verwendung ihrer personenbezogenen Daten zur Verfügung stellen. Diese Informationen müssen in knapper, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache bereitgestellt werden. Diese Informationen werden häufig in Form eines Datenschutzhinweises bereitgestellt. Wenn Kunden eine neue Technologie einsetzen (z. B. Copilot für Microsoft 365 oder Azure OpenAI Service) und beabsichtigen, diese Technologie auf eine Weise zu nutzen, die in den bestehenden Datenschutzhinweisen nicht berücksichtigt wird, müssen Sie Ihre Datenschutzhinweise aktualisiert wreden, um diese neuen Verarbeitungstätigkeiten zu berücksichtigen.

Die in diesem Paper sowie die unten aufgeführten Transparenz-Ressourcen enthaltenen Informationen sollen helfen zu verstehen, wie Copilot für Microsoft 365 und Azure OpenAI Service Daten verarbeiten und in welchem Umfang den betroffenen Personen gegebenenfalls zusätzliche Informationen mitgeteilt werden müssen. Zusätzliche produktspezifische Informationen finden sich unter

- Daten, Datenschutz und Sicherheit für Azure OpenAI Service
- Daten, Datenschutz und Sicherheit für Microsoft Copilot für Microsoft 365
- Copilot in Dynamics 365 und Power Platform
- FAQs für Copilot Datensicherheit und Datenschutz für Dynamics 365 und Power Platform.

## Artikel 15 bis 21 der DSGVO (Rechte der betroffenen Person)

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



Im Abschnitt „Rechte der betroffenen Personen; Unterstützung bei Anfragen“ des Datenschutzzusatzes (DPA) von Microsoft verpflichtet sich Microsoft, Kunden (in einer Weise, die mit der Funktionalität der Dienste und der Rolle von Microsoft als Datenverarbeiter vereinbar ist) die Möglichkeit zu bieten, Anfragen von betroffenen Personen zu erfüllen, die ihre Rechte gemäß der DSGVO ausüben.

Wenn Microsoft in Situationen, in denen es personenbezogene Daten im Namen von Unternehmen verarbeitet, eine solche Anfrage direkt von einer betroffenen Person erhält, leitet es die betroffene Person weiter, ihre Anfrage stattdessen an das Unternehmen selbst zu richten.

Sie sind für die Beantwortung solcher Anfragen verantwortlich, aber Microsoft wird diesbezüglich angemessene Unterstützungsanfragen erfüllen.

Microsoft hat zusätzliche Lösungen entwickelt, um seine Kunden bei der Beantwortung von Anfragen zu den Rechten der betroffenen Personen zu unterstützen, wie Microsoft Purview und Purview eDiscovery. Die Funktionen dieser Produkte versetzen Kunden in die Lage, ihre KI-Nutzung proaktiv zu steuern und sich an die sich entwickelnden gesetzlichen Anforderungen zu halten. Dies kann zum Beispiel wertvoll sein, um die Effizienz bei der Beantwortung und Bearbeitung von Anfragen im Zusammenhang mit dem „Recht auf Zugang zu personenbezogenen Daten“ und dem „Recht auf Vergessenwerden“ zu verbessern, die gemäß Artikel 15 und 17 der DSGVO gelten.

Mehr Informationen über Microsoft Purview und seine Funktionen und wie diese Tools bei der Bereitstellung der generativen KI-Lösungen von Microsoft unterstützen können.

## Artikel 28 der DSGVO (Pflichten des Auftragsverarbeiters)

Die DSGVO schreibt vor, dass eine Unternehmen, die als für die Verarbeitung Verantwortlicher fungiert, nur dann Datenverarbeiter mit der Verarbeitung personenbezogener Daten in ihrem Namen beauftragt, wenn diese ausreichend Garantien für die Erfüllung der wichtigsten Anforderungen der DSGVO bieten. Diese Hauptanforderungen sind in Artikel 28 beschrieben und beinhalten, dass sich die Datenverarbeiter zu Folgendem verpflichten:

+ dass Unterauftragsverarbeiter nur mit Zustimmung des für die Datenverarbeitung Verantwortlichen einsetzen und für Unterauftragsverarbeiter haften;
+ personenbezogene Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen zu verarbeiten, auch im Hinblick auf die Übermittlung;
+ sicherstellen, dass Personen, die personenbezogene Daten verarbeiten, zur Vertraulichkeit verpflichtet werden;
+ geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Niveau der Sicherheit personenbezogener Daten zu gewährleisten;
+ Unterstützung des für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen betroffener Personen auf Ausübung ihrer Rechte nach der DSGVO;
+ die Anforderungen der DSGVO in Bezug auf die Meldung von Datenschutzverletzungen und die Unterstützung erfüllen;

- Unterstützung des für die Datenverarbeitung Verantwortlichen bei Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden;
- personenbezogene Daten nach Beendigung der Erbringung von Dienstleistungen zu löschen oder zurückzugeben; und
- Unterstützung des für die Datenverarbeitung Verantwortlichen bei
- Nachweis der Einhaltung der DSGVO.

## Wie Microsoft seine Kunden unterstützt

Microsoft bietet die vertraglichen Verpflichtungen, die von Datenverarbeitern in Artikel 28 der DSGVO gegenüber seinen Kunden in Microsofts Datenschutzzusatz (DPA) (Data Protection Addendum, DPA). Diese spezifischen Verpflichtungen finden sich in der Anlage zur DPA mit dem Titel „European Union General Data Protection Regulation Terms“ (DSGVO der Europäischen Union), zusätzlich zum Hauptteil der DPA, der sich ausführlich mit den wesentlichen Anforderungen der DSGVO, einschließlich Artikel 28, befasst.

In diesem Zusammenhang ist es wichtig zu betonen, dass die DSGVO den für die Verarbeitung Verantwortlichen nicht vorschreibt, ihre eigenen Datenschutzbedingungen mit ihren Datenverarbeitern zu erstellen und zu verwenden. Der Europäische Datenschutzausschuss (EDPB) selbst erkennt an, dass die Verwendung der Standardbedingungen eines Cloud-Anbieters zulässig ist, sofern diese mit der DSGVO und Artikel 28[6] übereinstimmen.

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 bei Cloud-Diensten Standard und macht Cloud-Dienste verwaltbarer, skalierbarer, sicherer und kostengünstiger als Lösungen vor Ort. Bei einem mandantenfähigen Dienst kann sich eine von einem Kunden auferlegte Änderung auf alle Kunden auswirken, die den Dienst nutzen. Dies kann problematisch 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 insgesamt untergraben. Daher ist es für Microsoft nicht möglich, seine betrieblichen Abläufe zu ändern oder maßgeschneiderte vertragliche Verpflichtungen und / oder Vertragsstrukturen für einzelne Kunden zu schaffen.

Vor diesem Hintergrund müssen Kunden verstehen, dass die Schaffung eigener Datenverarbeitungsbedingungen bei der Zusammenarbeit mit Hyperscale-Cloud-Anbietern sie daran hindern kann, die reichhaltigen Innovationen der cloudbasierten generativen KI-Dienste zu nutzen.

[6] https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

## Artikel 32 der DSGVO (Technische und organisatorische Sicherheitsmassnahmen)

Nach Artikel 32 der DSGVO müssen die für die Verarbeitung Verantwortlichen sowie die Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen, um unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Maß an Sicherheit zu gewährleisten. Diese Maßnahmen sollten sich mit den Risiken befassen, die mit der versehentlichen oder unrechtmäßigen Zerstörung, dem Verlust, der Veränderung, der unbefugten Weitergabe von oder dem Zugang zu übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten verbunden sind.

### Wie Microsoft seine Kunden unterstützt

Im Abschnitt „Datensicherheit“ des Datenschutzzusatzes (DPA) von Microsoft verpflichtet sich Microsoft vertraglich, angemessene technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, um „Kundendaten“ und „personenbezogene Daten“ vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung, unbefugter Offenlegung oder unbefugtem Zugriff auf solche Daten, die übertragen, gespeichert oder anderweitig verarbeitet werden, zu schützen.

Diese technischen Maßnahmen sind in der Sicherheitspolitik von Microsoft dargelegt und entsprechen den Normen ISO 27001, ISO 27002 und ISO 27018. Microsoft verpflichtet sich außerdem vertraglich zur Verschlüsselung von „Kundendaten“ (einschließlich aller darin enthaltenen „personenbezogenen Daten“) bei der Übertragung (einschließlich zwischen Microsoft-Rechenzentren) und im Ruhezustand. Anhang A - Sicherheitsmaßnahmen zu Microsofts Datenschutzzusatz (DPA) enthält außerdem umfassende Verpflichtungen von Microsoft in Bezug auf die Sicherheit von Kundendaten, unter anderem in Bezug auf die Unternehmen der Informationssicherheit, die Verwaltung von Vermögenswerten, die Sicherheit der Human Ressources, die physische und ökologische Sicherheit, das Kommunikations- und Betriebsmanagement, die Informationssicherheit, das Incident-Management und das Management der Geschäftskontinuität.

Die oben beschriebenen technischen, organisatorischen und Sicherheitsmaßnahmen gelten für alle Kundendaten, die Kunden bereitstellen oder erstellen, wenn sie Copilot für Microsoft 365 und den Azure OpenAI-Dienst nutzen. Kunden können sich auf die oben dargelegten Informationen beziehen, um das Engagement und die Maßnahmen von Microsoft zum Schutz von Kundendaten (einschließlich personenbezogener Daten) zu demonstrieren.

Teil 3 enthält mehr Informationen zur Sicherheit von Copilot für Microsoft 365, Teil 4 mehr über die Sicherheit für den Azure Open AI Service.

## Artikel 35 der DSGVO (Datenschutz-Folgenabschätzungen)

Gemäß Artikel 35 der DSGVO müssen die für die Verarbeitung Verantwortlichen eine Datenschutz-Folgenabschätzung (Data Privacy Impact Assessment - DPIA) durchführen, wenn die Verarbeitung personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt (insbesondere, wenn dabei neue Technologien zum Einsatz kommen).

Bei der Beurteilung, ob eine Datenschutzfolgenabschätzung erforderlich ist, müssen die für die Verarbeitung Verantwortlichen die Art, den Umfang, den Inhalt und die Zwecke der Verarbeitung berücksichtigen. Ob eine Datenschutz-Folgenabschätzung für die Nutzung von Copilot für Microsoft 365 und Azure OpenAI Service erforderlich ist, hängt daher von dem jeweiligen Use Case und der Art der personenbezogenen Daten ab, die Kunden mit diesen Diensten verarbeiten möchten.

Mehr Informationen, wann eine Datenschutzfolgenabschätzung durchgeführt werden muss

Auch wenn sie nicht gesetzlich vorgeschrieben ist, ist eine Datenschutzfolgenabschätzung eine gute Praxis und kann dabei helfen, die spezifischen Datenschutzrisiken im Zusammenhang mit der Implementierung von Copilot für Microsoft 365 und / oder Azure OpenAI Service für einen bestimmten Use Case zu ermitteln. Die Erstellung einer Datenschutzfolgenabschätzung kann auch dabei helfen, Rechenschaftspflichten gemäß Artikel 5 Absatz 2 der DSGVO nachzukommen.

Eine DPIA muss mindestens enthalten:

+ eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung;
+ eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungen im Hinblick auf die Zwecke;
+ eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen; und
+ die geplanten Maßnahmen zur Bewältigung der Risiken, 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.

> Mehr Informationen über den Inhalt einer Data Privacy Impact Assessment - DPIA

### Wie Microsoft seine Kunden unterstützt

Die in diesem Paper enthaltenen Informationen sowie die zusätzlichen Ressourcen, auf die es verweist, können bei der Durchführung einer Datenschutzfolgenabschätzung helfen. Insbesondere die Informationen in:

+ Teil 3 und Teil 4, die sich darauf beziehen, wie Copilot für Microsoft 365 und Azure OpenAI Service Daten verarbeiten, helfen bei der Vervollständigung der oben unter a) beschriebenen Elemente; und
+ die Abschnitte über technische und organisatorische Maßnahmen sowohl für Copilot für Microsoft 365 als auch für Azure OpenAI Service helfen bei der Vervollständigung der oben unter d) beschriebenen Elemente.

Die unter den obigen Punkten beschriebenen Bewertungen sind von Fall zu Fall unterschiedlich und hängen vom jeweiligen Use Case sowie von Art, Umfang und Inhalt der betroffenen personenbezogenen Daten ab und müssen von Kunden selbst vorgenommen werden.

> Mehr Informationen über Data Protection Impact Folgenabschätzungen für die DSGVO

## Artikel 44 bis 50 der DSGVO (Übermittlung personenbezogener Daten in Drittländer)

Die DSGVO erlaubt die Übermittlung personenbezogener Daten in ein Drittland außerhalb der EU oder des EWR (einschließlich der USA), wenn bestimmte Bedingungen erfüllt sind.

Zu diesen Bedingungen gehört, dass ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt oder dass geeignete zusätzliche Schutzmaßnahmen (wie die EU-Standardvertragsklauseln) eingeführt wurden.

Für Kunden im Vereinigten Königreich erlaubt die britische Datenschutzverordnung die Übermittlung personenbezogener Daten in ein Drittland außerhalb des Vereinigten Königreichs (einschließlich der USA), wenn bestimmte Bedingungen erfüllt sind. Zu diesen Bedingungen gehört, dass ein Angemessenheitsbeschluss des britischen Außenministers vorliegt oder dass geeignete zusätzliche Garantien (wie das Addendum für die internationale Datenübermittlung zu den Standardvertragsklauseln der EU-Kommission („UK-Addendum“)) eingeführt worden sind.

### Wie Microsoft seine Kunden unterstützt

Alle Übermittlungen personenbezogener Daten durch Microsoft außerhalb des Vereinigten Königreichs, der EU oder des EWR unterliegen einem gültigen Übermittlungsmechanismus gemäß der DSGVO, einschließlich Übermittlungen in die USA.

Die EU-Kommission und das britische Außenministerium haben Angemessenheitsbeschlüsse bekannt gegeben, in denen festgestellt wird, dass (für die Zwecke von Artikel 45 der DSGVO) die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die aus dem Vereinigten Königreich oder der EU an Unternehmen in den USA übermittelt werden, die nach dem EU-U.S. Data Privacy Framework zertifiziert sind. Microsoft ist nach dem EU-U.S. Data Privacy Framework und den damit verbundenen Verpflichtungen zertifiziert. Microsoft hat sich verpflichtet, das Rahmenwerk zu übernehmen und wird darüber hinaus alle Anforderungen, die dieses Rahmenwerk für Kunden vorsieht, erfüllen oder übertreffen.

Microsoft verwendet auch weiterhin die EU-Standardvertragsklauseln und den britischen Zusatz, wo dies für Übertragungen aus dem Vereinigten Königreich, der EU oder Weiterübertragungen angemessen ist - zum VorTeil der Kunden und ihrer Rechtssicherheit bei Übertragungen, die ihren Ursprung in der EU haben.

Zusätzlich zu Microsofts konformen Datenübertragungsmechanismen hat Microsoft die EU Data Boundary eingerichtet und sich damit verpflichtet, die Daten seiner Kunden innerhalb der EU zu speichern und zu verarbeiten, wie in Microsofts Datenschutzzusatz (DPA) und den Microsoft-Produktbedingungen festgelegt, wodurch die Übermittlung personenbezogener Daten in Drittländer reduziert und die Einhaltung der DSGVO bei Übermittlungen in Drittländer vereinfacht wird. Sowohl Copilot für Microsoft 365 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 personenbezogener Daten) für bestimmte Online-Unternehmensdienste zu speichern und zu verarbeiten. Die EU- Datengrenze nutzt Microsoft-Rechenzentren, die in Österreich, Belgien, Dänemark, Finnland, Frankreich, Deutschland, Griechenland, Irland, Italien, den Niederlanden, Norwegen, Polen, Spanien, Schweden und der Schweiz angekündigt wurden oder derzeit betrieben werden, oder kann diese nutzen. In Zukunft kann Microsoft Rechenzentren in weiteren Ländern in der EU oder der EFTA einrichten, um EU Data Boundary-Dienste anzubieten.

Es gibt begrenzte Ausnahmen von der EU-Datengrenze, die dazu führen können, dass Microsoft Kundendaten (einschließlich personenbezogener Daten) außerhalb der EU-Datengrenze verarbeitet. Wenn dies der Fall ist, stützt sich Microsoft auf konforme Datenübertragungsmechanismen, wie sie in der DSGVO festgelegt sind. Weitere Einzelheiten zu diesen begrenzten Umständen finden sich in den Microsoft-Produktbedingungen.

> Mehr Informationen über die EU-Datenschutz-Grenze

Teil 3 enthält mehr Inforamtionen über Datenresidenz für Copilot für Microsoft 365, Teil 4 über Datenresidenz für Azure OpenAI Service zu erfahren.

## Wie interagiert die DSGVO mit dem KI-Gesetz?

Die DSGVO und das KI-Gesetz sollen sich gegenseitig ergänzen und einen Rechtsrahmen für KI-Produkte und -Dienste schaffen. Die DSGVO, welche die Verarbeitung personenbezogener Daten durch für die Verarbeitung Verantwortliche und Datenverarbeiter regelt, konzentriert sich auf den Datenschutz und zielt darauf ab, dem Einzelnen die Kontrolle über seine personenbezogenen Daten zu geben.

Das KI-Gesetz, das für Anbieter, Importeure, Vertreiber, Nutzer und andere am KI-Lebenszyklus Beteiligte gilt, soll sicherstellen, dass bei der Nutzung von KI-Systemen in der EU die Grundrechte, die Sicherheit und die ethischen Grundsätze gewahrt bleiben und bestimmte Risiken im Zusammenhang mit den leistungsfähigsten KI-Modellen für allgemeine Zwecke angegangen werden.

Weitere Informationen über das Gesetz über künstliche Intelligenz und sein Zusammenspiel mit der DSGVO finden sich in Anhang 2: Häufig gestellte Fragen (FAQs).

## Die kontinuierliche Einhaltung der Datenschutzbestimmungen und der offene Dialog mit den wichtigsten Aufsichtsbehörden in Europa und weltweit

Da sich die Gesetze zum Schutz der Privatsphäre und zum Datenschutz in Europa und auf der ganzen Welt weiterentwickeln, können Kunden sicher sein, dass Microsoft in Bezug auf Datenschutz-, Sicherheits- und Sicherungspraktiken transparent ist. Microsoft wird die Gesetze in Europa und weltweit einhalten, die KI regeln, und Versprechen mit klaren vertraglichen Verpflichtungen untermauern.

Über die Einhaltung der DSGVO und anderer für geltender gesetzlicher Vorschriften hinaus legt Microsoft großen Wert auf einen offenen Dialog mit seinen Kunden, Partnern und Aufsichtsbehörden, um die sich entwickelnden Bedenken in Bezug auf Datenschutz und Privatsphäre besser zu verstehen und anzugehen.

Microsoft arbeitet weiterhin eng mit Datenschutzbehörden und Regulierungsbehörden für den Schutz der Privatsphäre auf der ganzen Welt zusammen, um Informationen über die Funktionsweise von KI-Systeme auszutauschen und so ein Klima des Vertrauens und der Zusammenarbeit zu fördern.

# Teil 3: Copilot für Microsoft 365

Das Verständnis des Potenzials generativer KI-Dienste und der Art und Weise, wie diese Produkte und Dienste funktionieren und personenbezogene Daten verwenden, ist die Grundlage für die Einhaltung einer Reihe von Verpflichtungen im Rahmen der DSGVO. Dieser Teil 3 enthält Informationen und Links zu verschiedenen externen Ressourcen, die helfen können, die Funktionsweise von Copilot für Microsoft 365 zu verstehen, und bietet wichtige Informationen über das Produkt und seine Funktionen, die bei der Durchführung einer Datenschutzfolgenabschätzung oder einer anderen Datenschutzbewertung / -analyse helfen können.

## Was ist Copilot für Microsoft 365 und wie funktioniert es?

Copilot für Microsoft 365 ist ein KI-gestütztes Produktivitätstool, das „Large Language Models (LLMs)“ verwendet, um mit beliebten Microsoft 365-Apps wie Word, Excel, PowerPoint, Outlook, Teams und anderen zu arbeiten. Copilot für Microsoft 365 bietet intelligente Unterstützung in Echtzeit, die es Nutzern ermöglicht, ihre Kreativität, Produktivität und Fähigkeiten zu verbessern.

Copilot für Microsoft 365 basiert auf der gleichen Cloud-Infrastruktur wie Microsoft 365-Anwendungen und wendet die gleichen Grundsätze der Vertraulichkeit und des Datenschutzes für Kundendaten an, die Microsoft seit Jahren nutzt. Copilot für Microsoft 365 hält sich an alle bestehenden Datenschutz-, Sicherheits- und Compliance- Verpflichtungen, die für Microsoft 365 gelten, einschließlich Microsofts DSGVO-Verpflichtungen, wie in Microsofts Datenschutzzusatz (DPA) und in Bezug auf die EU-Datengrenze dargelegt.

Copilot für Microsoft 365 verwendet die organisatorischen Inhalte in Ihrem Microsoft 365-Tenant, einschließlich der Kalender, E-Mails, Chats, Dokumente, Besprechungen, Kontakte und mehr nur in Übereinstimmung mit den bestehenden Zugriffsrechten. Die Reichhaltigkeit der Copilot für Microsoft 365 Erfahrung hängt von den Datenquellen ab, die von Microsoft 365 indiziert werden. Kunden mit den umfangreichsten Daten in Microsoft 365 (Exchange, OneDrive, SharePoint, Teams) werden die besten Ergebnisse von Copilot erhalten. Durch den Zugriff auf umfassende Unternehmensdaten kann Copilot relevantere und personalisierte Inhalte vorschlagen, die auf dem Arbeitskontext und den Präferenzen des Nutzers basieren.

Copilot reagiert auf Aufforderungen der Benutzer. Ein „Prompt“ ist der Begriff, der beschreibt, wie Kunden Copilot für Microsoft 365 bitten, etwas für sie zu tun - wie z. B. Erstellen, Zusammenfassen, Bearbeiten oder Umwandeln. Ein Prompt ist wie ein Gespräch, bei dem eine einfache, aber klare Sprache verwendet und der Kontext angeben wird, wie man es mit einem Assistenten tun würden.

Wenn Copilot für Microsoft 365 Inhalte aus dem Microsoft 365-Tenant des Unternehmens verwendet, um die Prompt des Benutzers zu ergänzen und die Antwort zu bereichern, wie oben beschrieben, wird dies als „Grounding“ bezeichnet. Grounding ist etwas anderes als Training. Es werden keine Kundendaten verwendet, um den LLM zu trainieren. Tatsächlich ist der LLM zustandslos, d. h. er speichert weder Informationen über die Prompt, die ihm übermittelt wurde, noch über die Kundendaten, die für das Grounding verwendet wurden, noch über die von ihm gegebenen Antworten.

Copilot für Microsoft 365 nutzt eine Instanz einer Foundation LLM, die in Azure OpenAI gehostet wird. Copilot für Microsoft 365 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 Verwendung von Copilot für Microsoft 365 durch Ihr Unternehmen generiert werden, wie z. B. Prompts und Antworten - werden nicht ohne Ihre Zustimmung an Dritte weitergegeben.

Um die besten Antworten zu erhalten und das Beste aus Copilot für Microsoft 365 herauszuholen, ist es wichtig, dass Kunden geeignete Prompts eingeben und bestimmte häufige Fallstricke vermeiden. Mehr Informationen über die Kunst und Wissenschaft des Prompts (die Zutaten eines Prompts) und die Do‘s und Don‘ts der Prompts.

## Copilot für Microsoft 365 ist:

- die auf Microsofts umfassendem Ansatz für Sicherheit, Compliance und Datenschutz basiert;
- zum Schutz von Mieter-, Gruppen- und Individualdaten; und
- der verantwortungsvollen KI verpflichtet.

Informationen darüber, wie LLM funktioniert, wenn Kunden ihren Daten in Microsoft 365 verwenden: Mehr über Copilot für Microsoft 365.
Mehr Infos im Copilot-Labor, wie Copilot in bevorzugten Microsoft-Anwendungen eingesetzt werden können.
Ausführlichere Informationen über Copilot für Microsoft 365 finden sich auch im Microsoft Lernportal.

## Copilot und Ihre Privatsphäre

### Copilot unter Windows

Mehr Informationen, wie Copilot Kundendaten verwendet, um sie auf einem Windows-Gerät zu unterstützen.


### Copilot Pro (Heimanwender)

Mehr Informationen, wie Copilot Daten in Microsoft 365-Anwendungen zu Hause verwendet.

### Copilot für Microsoft 365 (IT-Profis / Admins)

Mehr Informationen, wie Unternehmensdaten verwendet und geschützt werden, wenn Copilot mit Microsoft 365 verwendet wird.

## Wie verwendet Copilot für Microsoft 365 persönliche Daten?

Copilot für Microsoft 365 bietet einen Mehrwert, indem es die LLMs von Microsoft mit Unternehmensdaten verbindet. Copilot für Microsoft 365 greift auf Inhalte und Kontext zu, um Antworten zu generieren, die in Unternehmensdaten verankert sind, wie z. B. Benutzerdokumente, E-Mails, Kalender, Chats, Meetings und Kontakte. Copilot für Microsoft 365 kombiniert diese Inhalte mit dem Arbeitskontext des Benutzers, wie z. B. der Besprechung, an der ein Benutzer gerade teilnimmt, dem E-Mail-Austausch des Benutzers zu einem Thema oder den Chat- Konversationen, die der Benutzer in einem bestimmten Zeitraum geführt hat. Copilot für Microsoft 365 nutzt diese Kombination aus Inhalt und Kontext, um genaue, relevante und kontextbezogene Antworten auf die Prompts des Benutzers zu geben.

Copilot für Microsoft 365 kann auf Webinhalte aus dem Bing-Suchindex verweisen, um Prompts und Antworten zu begründen. Basierend auf dem Prompt des Benutzers bestimmt Copilot für Microsoft 365, ob es Bing verwenden muss, um Webinhalte abzufragen, um dem Benutzer eine relevante Antwort zu geben. Es sind Steuerelemente verfügbar, um die Verwendung von Webinhalten für Administratoren zu verwalten.

Die Missbrauchsüberwachung für Copilot für Microsoft 365 erfolgt in Echtzeit, ohne dass Microsoft einen ständigen Zugriff auf die Kundendaten erhält, weder für eine menschliche noch für eine automatische Überprüfung. Während die Missbrauchsmoderation, die eine menschliche Überprüfung von Inhalten beinhaltet, für Azure OpenAI Service verfügbar ist, ist dies für Copilot für Microsoft 365 nicht erforderlich.

Microsoft wird Daten über Benutzerinteraktionen mit Copilot für Microsoft 365 sammeln und speichern. Dazu gehören die Prompt des Benutzers, die Reaktion von Copilot und die Informationen, die zur Begründung der Copilot- Antwort verwendet werden („Inhaltsinteraktionen“). Kundenadministratoren können die Inhaltsinteraktionen ihrer Unternehmen anzeigen, verwalten und durchsuchen. Es kann notwendig sein, die Datenschutzhinweise für die Nutzer der Unternehmen zu aktualisieren, um sicherzustellen, dass die Verarbeitung personenbezogener Daten durch Administratoren in diesem Zusammenhang angemessen erfasst wird. In Teil 2 finden sich weitere Einzelheiten zu den Transparenzverpflichtungen gemäß der DSGVO.

Für Microsoft ist es wichtig, dass die Daten der Kunden den Kunden gehören. Microsoft erhebt keinen Anspruch auf das Eigentum an den von Copilot für Microsoft 365 erstellten Inhalten. Alle Inhaltsinteraktionen, einschließlich der Prompts und aller Ausgabedaten / -inhalte, gelten als „Kundendaten“ in den Produktbedingungen und dem Datenschutzzusatz (DPA) von Microsoft.

Alle von Copilot für Microsoft 365 verarbeiteten Kundendaten werden in Übereinstimmung mit den vertraglichen Verpflichtungen mit den anderen Inhalten Ihres Unternehmens in Microsoft 365 verarbeitet und gespeichert.

Copilot für Microsoft 365 verwendet keine Kundendaten zum Trainieren von Basismodellen ohne die Zustimmung der Kunden.

## Sicherheit für Copilot für Microsoft 365

Wie in Teil 2 erwähnt, verpflichtet die DSGVO die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein gewisses Maß an Sicherheit für alle von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten.

Für Copilot für Microsoft 365 gelten standardmäßig dieselben Sicherheits- und Compliance-Bedingungen, die bereits für die Nutzung von Microsoft 365 durch Ihr Unternehmen gelten. Copilot für Microsoft 365 wird in der Azure-Infrastruktur gehostet und ist durch einige der umfassendsten Compliance- und Sicherheitskontrollen für Unternehmen in der Branche geschützt. Copilot für Microsoft 365 wurde entwickelt, um die Vorteile der Sicherheits- und Compliance-Funktionen zu nutzen, die in Microsofts Hyperscale-Cloud bereits gut etabliert sind. Dazu gehört die Priorisierung von Zuverlässigkeit, Redundanz, Verfügbarkeit und Skalierbarkeit, die alle standardmäßig in den Cloud-Diensten enthalten sind.

Copilot für Microsoft 365 respektiert auch die Zugriffsberechtigungen jedes Benutzers für alle Inhalte, die es abruft. Dies ist wichtig, da Copilot für Microsoft 365 nur Antworten generiert, die auf Informationen basieren, für die der jeweilige Benutzer eine Zugriffsberechtigung hat.

Microsoft implementiert bereits mehrere Formen des Schutzes, um Kunden daran zu hindern, Microsoft 365-Dienste und -Anwendungen zu kompromittieren oder sich unbefugten Zugang zu anderen Tenants oder dem Microsoft 365- System selbst zu verschaffen.

## Im Folgenden werden einige Beispiele für diese Formen des Schutzes genannt:

- Die logische Isolierung von Kundendaten innerhalb jedes Mandanten für Microsoft 365-Dienste wird durch Microsoft Entra-Autorisierung und rollenbasierte Zugriffskontrolle erreicht. Mehr Informationen über Microsoft 365 Isolationskontrollen.
- Microsoft verwendet strenge physische Sicherheitsmaßnahmen, Hintergrundüberprüfungen und eine mehrschichtige Verschlüsselungsstrategie, um die Vertraulichkeit und Integrität der Kundendaten zu schützen.
- Microsoft 365 verwendet dienstseitige Technologien, die Kundendaten sowohl im Ruhezustand als auch bei der Übertragung verschlüsseln, einschließlich BitLocker, Verschlüsselung pro Datei, Transport Layer Security (TLS) und Internet Protocol Security (IPsec). Weitere Informationen zur Verschlüsselung in Microsoft 365 finden sich unter Verschlüsselung in der Microsoft Cloud.
- Die Kontrolle über die Daten Ihres Unternehmens wird durch die Verpflichtung von Microsoft zur Einhaltung allgemein geltender Datenschutzgesetze, einschließlich der DSGVO, und von Datenschutzstandards wie ISO / IEC 27018, dem weltweit ersten internationalen Verhaltenskodex für den Datenschutz in der Cloud, verstärkt.
- Für Inhalte, auf die über Copilot für Microsoft 365-Plug-ins zugegriffen wird, kann die Verschlüsselung den programmatischen Zugriff ausschließen und so den Zugriff des Plug-ins auf den Inhalt beschränken. Mehr Informationen über das Konfigurieren von Nutzungsrechten für Azure Information Protection.
- Da es sich bei generativen KI-Systemen auch um Softwaresysteme handelt, kommen alle Elemente des Sicherheitsentwicklungszyklus zur Anwendung: von der Bedrohungsmodellierung über die statische Analyse, die sichere Erstellung und den sicheren Betrieb bis hin zur Verwendung starker Kryptografie, Identitätsstandards und mehr.
- Microsoft hat auch neue Schritte zum Security Development Lifecycle hinzugefügt, um sich auf KI- Bedrohungsvektoren vorzubereiten, einschließlich der Aktualisierung der SDL-Anforderung zur Bedrohungsmodellierung, um KI- und Machine-Learning-spezifische Bedrohungen zu berücksichtigen. Microsoft hat seine KI-Produkte einem KI-Red-Teaming unterzogen, um nach Schwachstellen zu suchen und sicherzustellen, dass Microsoft über geeignete Strategien zur Risikominderung verfügt.

## EU-Datengrenze und Datenresidenz

Wie in Teil 2 dieses Papers erklärt, ist Copilot für Microsoft 365 ein EU Data Boundary Service. Mehr Informationen

Wenn Daten, die von Copilot für Microsoft 365 generiert wurden, in Microsoft 365-Produkten gespeichert werden, für die bereits Verpflichtungen zur Datenresidenz gemäß den Produktbedingungen bestehen, werden die geltenden Verpflichtungen eingehalten.

Copilot für Microsoft 365 wurde als betroffener Worklad in die Verpflichtungen zur Datenaufbewahrung in den Microsoft-Produktbedingungen aufgenommen. Die Angebote Advanced Datenresidenz (ADR) und Multi-Geo Capabilities von Microsoft enthalten ebenfalls Verpflichtungen zur Datenresidenz für Copilot für Microsoft 365-Kunden.

# Teil 4: Azure OpenAI Dienst

Zu verstehen, wie generative KI-Produkte und -Dienste funktionieren und personenbezogene Daten verwenden, ist die Grundlage für die Einhaltung einer Reihe von Verpflichtungen gemäß der DSGVO. Dieser Teil 4 enthält Informationen und Links zu verschiedenen externen Ressourcen, die helfen können, die Funktionsweise des Azure OpenAI Service zu verstehen, und bietet wichtige Informationen über den Dienst und seine Funktionen, die bei der Durchführung einer Datenschutzfolgenabschätzung oder einer anderen Datenschutzbeurteilung / -analyse hilfreich sein können.

## Was ist der Azure OpenAI Service und wie funktioniert es?

Azure OpenAI Service ist eine Cloud-basierte Plattform, die es Kunden ermöglicht, ihre eigenen generativen KI- Anwendungen zu entwickeln und einzusetzen und dabei die Leistungsfähigkeit von KI-Modellen zu nutzen. Azure OpenAI Service bietet Kunden Zugang zu einer Reihe von LLMs für die Entwicklung von generativen KI-Erfahrungen.

Von der Generierung realistischer Bilder und Videos bis hin zur Verbesserung des Kundenerlebnisses hat sich generative KI als vielseitiges Werkzeug in verschiedenen Branchen bewährt. Die Modelle, die dem Azure OpenAI Service zugrunde liegen, können leicht an die spezifische Aufgabe angepasst werden, z. B.: Entwurf, Erstellung und Generierung von Inhalten, Zusammenfassung, semantische Suche, Übersetzung von natürlicher Sprache in Code, beschleunigte Automatisierung, personalisiertes Marketing, Chatbots und virtuelle Assistenten, Produkt- und Dienstleistungsinnovation, Sprachübersetzung und natürliche Sprachverarbeitung, Betrugserkennung und Cybersicherheit, prädiktive Analysen und Prognosen, kreatives Schreiben sowie medizinische Forschung und Diagnose.

Der Azure OpenAI Service wird vollständig von Microsoft kontrolliert. Microsoft hostet die OpenAI / Chat GPT-Modelle in Microsofts Azure-Umgebung und der Dienst interagiert nicht mit den von OpenAI betriebenen Diensten (z. B. ChatGPT oder die OpenAI-API).

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

OpenAI / ChatGPT ist kein Unterauftragsverarbeiter von Microsoft und Kundendaten - einschließlich der Daten, die durch die Nutzung des Azure OpenAI Service durch Ihr Unternehmen generiert werden, wie z. B. Prompts und Antworten - werden vertraulich behandelt und nicht ohne Ihre Zustimmung an Dritte weitergegeben.

> Mehr Informationen über die zugrunde liegenden LLMs, die den Azure OpenAI Dienst ermöglichen

## Azure OpenAI Service kann auf folgende Weise genutzt werden:

+ **Prompt-Engineering** ist eine Technik, bei der Prompts für LLMs entworfen werden. Die Prompts werden vom Benutzer eingereicht, und der Inhalt wird vom Dienst über die Operationen Vervollständigungen, Chatvervollständigungen, Bilder und Einbettungen generiert. Dieser Prozess verbessert die Genauigkeit und Relevanz der Antworten und optimiert die Leistung des Modells.

> Mehr Informationen über Prompt Engineering.

+ **Azure OpenAI auf Ihren Daten:** Wenn Kunden die Funktion „on your data“ verwenden, ruft der Service relevante Daten aus einem konfigurierten Kundendatenspeicher ab und erweitert die Prompt, um Generationen zu erzeugen, die mit Kundendaten grounded sind. Azure OpenAI „on your data“ ermöglicht es, unterstützte LLMs auf den Unternehmensdaten auszuführen, ohne dass Kunden Modelle trainieren oder feinabstimmen müssen. Die Ausführung von Modellen auf Kundendaten ermöglicht es, Daten mit größerer Genauigkeit und Geschwindigkeit zu analysieren. Auf diese Weise können wertvolle Erkenntnisse gewonnen werden, die helfen, bessere Entscheidungen zu treffen, Trends und Muster zu erkennen und Abläufe zu optimieren. Einer der Hauptvorteile von Azure OpenAI „on your data“ ist die Möglichkeit, den Inhalt der Konversations-KI anzupassen. Das Modell innerhalb des Azure OpenAI Service hat Zugriff auf spezifische Quellen und kann auf diese verweisen, um die Antworten zu unterstützen. Die Antworten basieren nicht nur auf dem vortrainierten Wissen des Modells, sondern auch auf den neuesten Informationen, die in der jeweiligen Datenquelle verfügbar sind. Diese Basisdaten helfen dem Modell auch dabei, Antworten zu vermeiden, die auf veralteten oder falschen Informationen basieren.

> Mehr Informationen über Azure OpenAI On Your Data

+ Mit Azure OpenAI-Feinabstimmung können Kunden ihre eigenen Trainingsdaten, bestehend aus Prompts- Ausfüllungspaaren, für die Feinabstimmung eines OpenAI-Modells bereitstellen. Dieser Prozess dient der Feinabstimmung eines bestehenden LLM anhand von Beispieldaten. Diese Feinabstimmung bezieht sich auf den Prozess des erneuten Trainings von zuvor trainierten Modellen auf bestimmten Datensätzen, typischerweise um die Leistung des Modells bei bestimmten Aufgaben zu verbessern oder Informationen einzubringen, die beim ursprünglichen Training des Basismodells nicht gut repräsentiert wurden. Das Ergebnis ist ein neues „kundenspezifisches“ LLM, das anhand der bereitgestellten Beispiele für den Kunden optimiert wurde. Trainingsdaten und fein abgestimmte Modelle

  1. sind ausschließlich für die Nutzung durch das Unternehmen verfügbar.
  2. Werden in derselben Region wie die Azure OpenAI-Ressource gespeichert.
  3. können vom Kunden jederzeit gelöscht werden.

Wenn benutzerdefinierte Daten hochgeladen werden, um die Ergebnisse des LLM zu verfeinern, werden sowohl die Kundendaten als auch die Ergebnisse des verfeinerten Modells in einem geschützten Bereich der Cloud aufbewahrt, der in einem Tenant gespeichert ist - nur für das Unternehmen zugänglich und durch robuste Kontrollen getrennt, um jeden anderen Zugriff zu verhindern. Die Kundendaten und -Ergebnisse können zusätzlich entweder durch von Microsoft verwaltete oder vom Kunden verwaltete Verschlüsselungsschlüssel in einem „Bring Your Own Key“-Format verschlüsselt werden, wenn der Kunde dies wünscht. In den meisten Fällen kann Microsoft Support leisten und Probleme mit dem Dienst beheben, ohne auf Kundendaten zugreifen zu müssen (z. B. auf die Daten, die zur Feinabstimmung hochgeladen wurden). In den seltenen Fällen, in denen ein Zugriff auf Kundendaten erforderlich ist, sei es als Reaktion auf ein vom Kunden initiiertes Support-Ticket oder auf ein von Microsoft identifiziertes Problem, können Kunden mit Customer Lockbox für Microsoft Azure die Kontrolle über den Zugriff auf diese Daten übernehmen. Customer Lockbox gibt Kunden die Möglichkeit, jede Zugriffsanfrage auf ihre Kundendaten zu genehmigen oder abzulehnen.

> Mehr Informationen über die Feinabstimmung von Azure OpenAI

Unabhängig davon, ob die Inhalte als Grundlage für die Prompts mit der Funktion „Eigene Daten“ verwendet werden oder ob die Inhalte zum Aufbau eines Feinabstimmungsmodells verwendet werden, werden die Kundendaten nicht zum Trainieren des LLM verwendet. Tatsächlich ist das LLM zustandslos, d. h. es speichert weder Informationen über die Prompts, die ihm übermittelt wurden, noch über die Kundendaten,

die als Grundlage verwendet wurden, noch über die von ihm gegebenen Antworten. Das LLM wird nicht trainiert und lernt zu keinem Zeitpunkt während dieses Prozesses, es ist genau dasselbe Basismodell, auch nachdem Millionen von Prompts ausgeführt wurden.

> Ausführliche Informationen zu den Azure OpenAI Services finden sich in der Azure OpenAI Service - Dokumentation, Quickstarts und API-Referenzhandbüchern.

## Verhinderung von Missbrauch und der Erstellung schädlicher Inhalte

Um das Risiko einer schädlichen Nutzung des Azure OpenAI Service zu verringern, sind sowohl Funktionen zur Inhaltsfilterung als auch zur Missbrauchsüberwachung enthalten.

Unter Inhaltsfilterung versteht man den Prozess, bei dem Antworten synchron mit automatischen Mitteln geprüft werden, um festzustellen, ob sie gefiltert werden sollten, bevor sie an den Benutzer zurückgesendet werden. Diese Prüfung erfolgt, ohne dass Daten gespeichert werden müssen, und ohne dass ein Mensch die Prompts (d. h. den von den Nutzern als Anfragen bereitgestellten Text) oder die Antworten (d. h. die an den Nutzer zurückgesandten Daten) überprüft.

> Mehr Informationen über die Filterung von Inhalten

Die Missbrauchsüberwachung wird durch einen separaten Prozess durchgeführt. Auf diese Daten dürfen nur autorisierte Microsoft-Mitarbeitende zugreifen, um die Fehlersuche zu unterstützen und das System vor Missbrauch zu schützen. Bei den menschlichen Überprüfern handelt es sich um autorisierte Microsoft-Mitarbeitende, die über punktuelle Abfragen unter Verwendung von Anforderungs-IDs, Secure Access Workstations (SAWs) und Just-In-Time (JIT)-Anforderungsgenehmigungen durch Teamleiter auf die Daten zugreifen.

> Mehr Informationen zur Missbrauchsüberwachung

Diese menschliche Überprüfung kann eine Herausforderung für Kunden darstellen, die ein Gleichgewicht zwischen der Sicherheit des Systems und den Risiken eines externen Zugriffs - selbst unter kontrollierten Bedingungen - finden müssen. Um dieses Gleichgewicht herzustellen, bietet Microsoft Funktionen für den eingeschränkten Zugriff an, mit denen genehmigte Kunden-Nutzungsfälle von diesen menschlichen Überprüfungs- und Datenprotokollierungsprozessen ausgenommen werden können.

Einige Kunden möchten den Azure OpenAI Service möglicherweise für einen Use Case nutzen, der die Verarbeitung sensibler, streng vertraulicher oder gesetzlich geregelter Eingabedaten beinhaltet, bei dem die Wahrscheinlichkeit schädlicher Ausgaben und / oder eines Missbrauchs jedoch gering ist. Diese Kunden können zu dem Schluss kommen, dass sie aufgrund ihrer internen Richtlinien oder des geltenden Rechts nicht wollen oder nicht das Recht haben, Microsoft die Verarbeitung solcher Daten zur Missbrauchserkennung, wie oben beschrieben, zu gestatten. Um diese Bedenken auszuräumen, erlaubt Microsoft Kunden, die zusätzliche Kriterien für den eingeschränkten Zugang erfüllen und bestimmte Use Cases nachweisen können, die Deaktivierung der Azure OpenAI Content Management- Funktionen zu beantragen, indem sie dieses Formular ausfüllen.

Wenn Microsoft die Anforderung eines Kunden, die Missbrauchsüberwachung zu deaktivieren, genehmigt, speichert Microsoft keine Prompts und Abschlüsse, die mit dem genehmigten Azure-Abonnement verbunden sind, für das die Missbrauchsüberwachung deaktiviert ist. Da in diesem Fall keine Prompts und Abschlüsse im Speicher für Dienstergebnisse gespeichert werden, ist der menschliche Überprüfungsprozess nicht möglich und wird nicht durchgeführt.

## Wie verwendet der Azure OpenAI Service personenbezogene Daten?

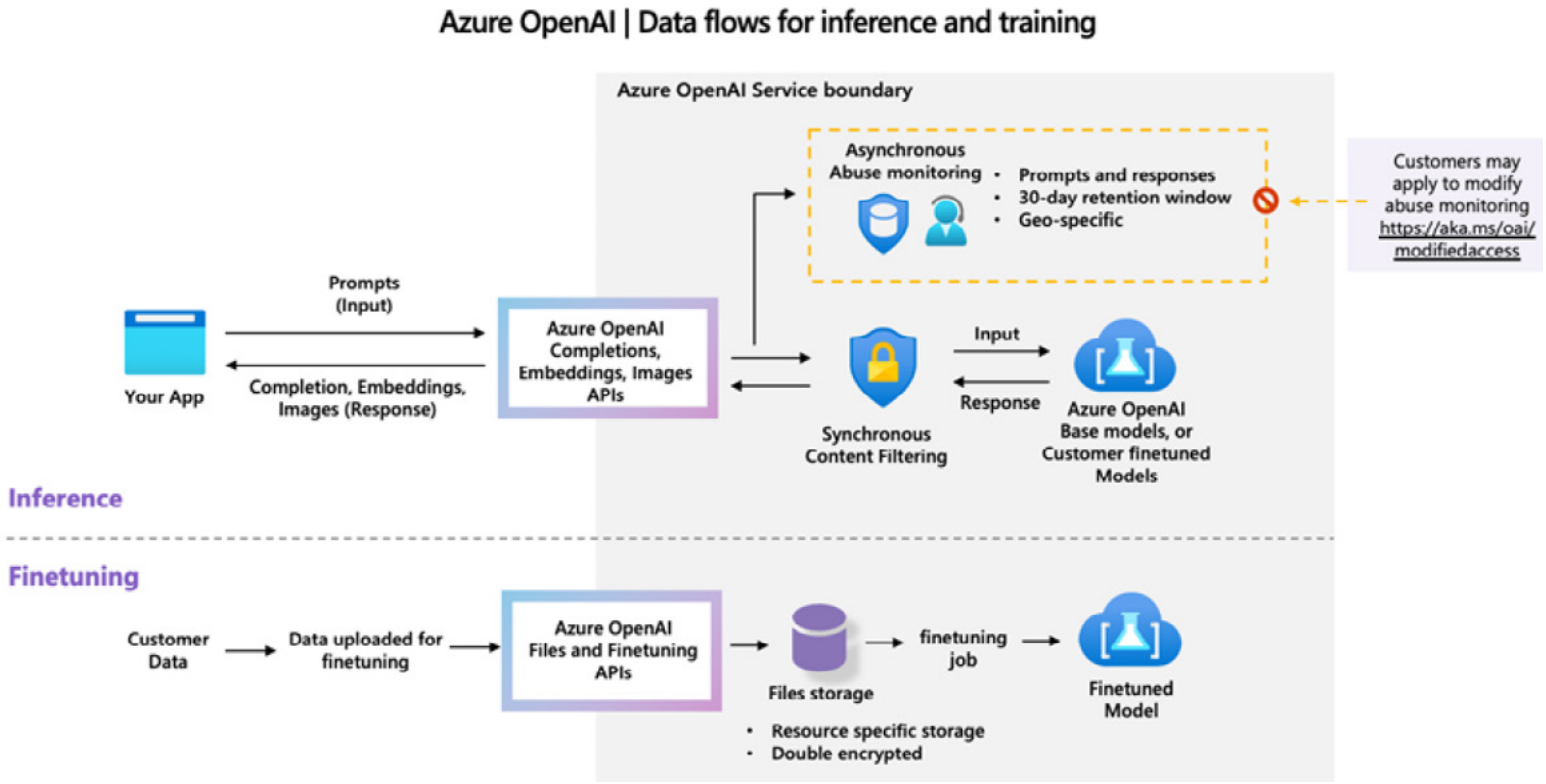
Das folgende Diagramm veranschaulicht, wie die Daten eines Unternehmens vom Azure OpenAI Service verarbeitet werden. Dieses Diagramm umfasst drei verschiedene Arten der Verarbeitung:

1. Wie Azure OpenAI Service Prompts verarbeitet, um Inhalte zu generieren (einschließlich, wenn zusätzliche Daten aus einer verbundenen Datenquelle zu einem Prompt mit Azure OpenAI „On Your Data“ hinzugefügt werden).
2. Wie Azure OpenAI Service ein fein abgestimmtes (benutzerdefiniertes) Modell mit Ihren Trainingsdaten erstellt.
3. Wie der Azure OpenAI-Dienst und Microsoft-Mitarbeitende Prompts, Vervollständigungen und Bilder auf schädliche Inhalte und auf Muster analysieren, die auf eine Nutzung des Dienstes in einer Weise hindeuten, die gegen den Verhaltenskodex oder andere geltende Produktbedingungen verstößt.

Prompts (Eingaben) und Vervollständigungen (Ausgaben), Einbettungen und Trainingsdaten:

- sind NICHT für andere Kunden verfügbar.
- sind für OpenAI NICHT verfügbar.
- werden NICHT ohne die Zustimmung des Kunden für das Training von Basismodellen verwendet.
- werden NICHT zur Verbesserung von Produkten oder Diensten von Microsoft oder Drittanbietern verwendet.
- werden NICHT für die automatische Verbesserung von Azure OpenAI-Modellen für die Verwendung in Ihrer Ressource verwendet (die Modelle sind zustandslos, es sei denn, Kunden nehmen explizit eine Feinabstimmung der Modelle mit Trainingsdaten vor).

Auf den Kunden abgestimmte Azure OpenAI-Modelle sind exklusiv für die Nutzung durch ihr Unternehmen verfügbar.



## Sicherheit für Azure OpenAI

Wie in Teil 2 dieses Papers dargelegt, verpflichtet die DSGVO die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein gewisses Maß an Sicherheit für alle von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten.

Die Sicherheit ist in den gesamten Entwicklungszyklus aller Microsoft Unternehmensdienste (einschließlich derjenigen, die generative KI-Technologie enthalten) integriert, von der Konzeption bis zur Bereitstellung.

Azure OpenAI Service wird in der Azure-Infrastruktur gehostet und ist durch einige der umfassendsten Compliance- und Sicherheitskontrollen für Unternehmen in der Branche geschützt. Diese Dienste wurden entwickelt, um die Vorteile der Sicherheits- und Compliance-Funktionen zu nutzen, die in Microsofts Hyperscale-Cloud bereits gut etabliert sind.

Dazu gehört die Priorisierung von Zuverlässigkeit, Redundanz, Verfügbarkeit und Skalierbarkeit, die alle standardmäßig in Cloud-Services integriert sind.

Da es sich bei generativen KI-Systemen auch um Softwaresysteme handelt, kommen alle Elemente des Security Development Lifecycle zur Anwendung: von der Bedrohungsmodellierung über die statische Analyse, die sichere Erstellung und den sicheren Betrieb bis hin zur Verwendung starker Kryptografie und Identitätsstandards.

Microsoft hat auch neue Schritte zum Security Development Lifecycle hinzugefügt, um sich auf KI- Bedrohungsvektoren vorzubereiten, einschließlich der Aktualisierung der SDL-Anforderung zur Bedrohungsmodellierung, um KI- und Machine-Learning-spezifische Bedrohungen zu berücksichtigen. Microsoft hat seine KI-Produkte einem KI-Red-Teaming unterzogen, um nach Schwachstellen zu suchen und zu bestätigen, dass Microsoft über angemessene Strategien zur Risikominderung verfügt.

> Mehr Informationen über Daten, Datenschutz und Sicherheit für Azure OpenAI Service

## EU-Datengrenze und Datenresidenz

Azure OpenAI Service ist ein EU Data Boundary Service. Für die Zwecke der Auslegung des Abschnitts „EU Data Boundary Services“ der Produktbedingungen ist der Azure OpenAI Service ein Azure Service, der den Einsatz in einer Region innerhalb der EU Data Boundary ermöglicht.

> Mehr Informationen über die EU-Datengrenze

In Zusammenhang mit:

+ **Azure OpenAI auf Daten-Funktion:** Alle Datenquellen, die Kunden als Grundlage für die generierten Ergebnisse bereitstellen, bleiben in der von ihnen angegebenen Datenquelle und an dem von ihnen angegebenen Ort gespeichert. Es werden keine Daten in den Azure OpenAI-Service kopiert.
+ **Trainingsdaten und Feinabstimmung (benutzerdefinierte) LLMs:** Diese werden in der gleichen Region wie die Azure OpenAI-Ressource im Azure-Tenant des Kunden gespeichert.
+ **Missbrauchsüberwachung für Kunden, die den Azure OpenAI-Dienst in Europa nutzen:** Diese Überprüfung wird ausschließlich von Microsoft-Mitarbeitenden im Europäischen Wirtschaftsraum durchgeführt. Der Datenspeicher, in dem Prompts und Vervollständigungen gespeichert werden, ist logisch nach Kundenressourcen getrennt (jede Anfrage enthält die Ressourcen-ID der Azure OpenAI-Ressource des Kunden). Ein separater Datenspeicher befindet sich in jeder Region, in der der Azure OpenAI-Service verfügbar ist, 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: Schlussfolgerung

Microsoft lebt vom Vertrauen. Microsoft hat bei allem, was sie tun, der Sicherheit, dem Datenschutz und der Einhaltung von Vorschriften verpflichtet, und sein Ansatz für generative KI ist nicht anders. Als Branchenführer bei der Bereitstellung von generativen KI-Lösungen vertrauen den Kunden auf der ganzen Welt und Microsoft hält sich an die strengsten Datenschutz- und Sicherheitsstandards der Branche. Microsoft bietet seinen Kunden erstklassige Produkte und Dienstleistungen und unterstützen sie so bei der Verwirklichung ihrer Ziele für die digitale Transformation.

Außerdem hat Microsoft seinen Kunden bewusst seiene Bereitschaft und sein Engagement signalisiert, seine Datenschutz- und Privatsphäre-Einstellungen richtig zu machen, um die Einhaltung der DSGVO zu gewährleisten. Microsoft demonstriert dieses Engagement durch Verträge, eine umfangreiche technische Dokumentation (mit Details zu Datenprozessen und -aktivitäten) und die Implementierung technischer und organisatorischer Schutzmaßnahmen, um verbleibende Datenschutz- und Sicherheitsrisiken zu minimieren. Unterstützt wird dies durch die konsequente Einbindung von Regulierungsbehörden und Branchenvertretern, mit denen Microsoft auf seinem Weg zu Verantwortung, Rechenschaftspflicht und Integrität bei der Bereitstellung generativer KI-Lösungen im großen Maßstab zusammenarbeiten.

Während sich die regulatorische Landschaft weiterentwickelt und Microsoft neue Arten von KI-Lösungen anbietet, ist Microsoft bewusst, dass Unternehmen weiterhin auf die Hilfe bei der Entschlüsselung und Operationalisierung der Anforderungen neuer und bestehender Datenschutzrahmen angewiesen sein werden. Microsoft wird weiterhin branchenführende Tools, Transparenz-Ressourcen und Unterstützung anbieten und Microsoft freut sich auf die Gelegenheit, anhaltendes Engagement für die Bedürfnisse und Anforderungen der europäischen Kunden auf ihrem Weg zur KI zu demonstrieren.

# Anhang 1: Geschäftsmöglichkeiten, die sich aus generativer KI ergeben

Die Verfügbarkeit von generativen KI-Lösungen hat die Überlegungen zu generativen KI-Use Casesn beschleunigt. In diesem Anhang werden mehrere relevante Bereiche aufgeführt, die von Unternehmen in Betracht gezogen werden sollten.

## Möglichkeiten der KI-Transformation

Die Integration von generativer KI in den Geschäftsbetrieb wird durch mehrere wichtige Möglichkeiten vorangetrieben:

- **Bessere Erfahrungen für Mitarbeitende:** Durch die Automatisierung von routinemäßigen und zeitaufwändigen Aufgaben werden PersonalRessourcen freigesetzt, um sich auf strategischere Initiativen zu konzentrieren. KI-gesteuerte Prozesse reduzieren menschliche Fehler und erhöhen die Präzision der Ergebnisse, von Finanzprognosen bis hin zu Prüfungen der Einhaltung gesetzlicher Vorschriften.
- **Kundenbindung neu erfinden:** Durch personalisierte Erlebnisse und schnelle Antworten auf Kundenanfragen kann KI dazu beitragen, die allgemeine Kundenzufriedenheit und -treue zu verbessern.
- **Geschäftsprozesse umgestalten:** Wenn Unternehmen wachsen, kann KI problemlos skaliert werden, um das wachsende Daten- und Transaktionsvolumen zu bewältigen und eine konsistente Leistung ohne proportionalen Anstieg der Betriebskosten zu gewährleisten.
- **Ermöglichen von Innovation:** KI erleichtert die Erkundung neuer Geschäftsmodelle und Dienstleistungen, indem KI eingesetzt wird, um Trends zu erkennen, Marktbewegungen vorherzusagen und Angebote anzupassen.

Diese Einführung bildet die Grundlage für eine detaillierte Untersuchung der spezifischen Anwendungen der generativen KI in verschiedenen Branchen und zeigt, dass ihre Fähigkeiten nicht nur theoretisch sind, sondern praktische und transformative Auswirkungen auf die Geschäftsabläufe haben.

## Allgemeine Use Cases für Copilot für Microsoft 365

Copilot für Microsoft 365 wurde entwickelt, um die betriebliche Effizienz und die Entscheidungsfindung in einer Vielzahl von Branchen zu verbessern. Dieser Abschnitt skizziert die beliebtesten und universell einsetzbaren Use Cases für

Copilot für Microsoft 365 und demonstriert damit seine Flexibilität und den Mehrwert für jeden Geschäftsbetrieb.

+ **Automatisierter Kundensupport:** fortschrittliche virtuelle Assistenten und Chatbots, die Kundenanfragen verwalten, Echtzeit-Support bieten und Probleme selbstständig lösen. Dies verkürzt die Reaktionszeiten, erhöht die Kundenzufriedenheit und senkt die Betriebskosten, die mit der Unterhaltung großer Kundendienstteams verbunden sind.
+ **Automatisierung und Verwaltung von Dokumenten:** Erstellen, formatieren und verwalten Sie Dokumente. Copilot für Microsoft 365 kann auf der Grundlage von Benutzereingaben Berichte erstellen, Korrespondenz entwerfen und Präsentationen vorbereiten. Dies steigert die Produktivität und sorgt für Konsistenz in der gesamten Unternehmenskommunikation, so dass sich die Mitarbeitenden auf strategischere Aufgaben konzentrieren können.
+ **Datenanalyse und Gewinnung von Erkenntnissen:** Analyse großer Datensätze zur Ermittlung von Trends, Durchführung von prädiktiven Analysen und Gewinnung verwertbarer Erkenntnisse, die für die Entscheidungsfindung entscheidend sind. Dies hilft Unternehmen, fundierte Entscheidungen auf der Grundlage datengestützter Erkenntnisse zu treffen, den Betrieb zu optimieren und die strategische Planung zu verbessern.
+ **Workflow- und Prozessautomatisierung:** Automatisieren Sie sich wiederholende und zeitraubende Aufgaben wie Dateneingabe, Terminplanung und Prozessverfolgung und integrieren Sie sie nahtlos in bestehende Systeme, um Arbeitsabläufe zu optimieren. Dies steigert die betriebliche Effizienz, reduziert menschliche Fehler und gibt den Mitarbeitenden die Möglichkeit, sich auf höherwertige Tätigkeiten zu konzentrieren.
+ **Personalisierte Inhalte und Empfehlungen:** Copilot für Microsoft 365 schneidet Inhalte und Empfehlungen auf einzelne Benutzer zu, basierend auf ihrem Verhalten, ihren Vorlieben und früheren Interaktionen, wie sie in Bereichen wie E-Commerce, Medien und Content Delivery üblich sind. Dies steigert das Engagement und die Zufriedenheit der Benutzer, was zu einer höheren Loyalität und einem höheren Umsatz durch personalisierte Erlebnisse führt.

## Abteilungs- und Mitarbeitendenspezifische Use Cases

Wir haben die Microsoft Copilot-Szenariobibliothek entwickelt, um Anleitungen für abteilungs- und Mitarbeitendenspezifische Szenarien zur Verfügung zu stellen, damit Sie sich inspirieren lassen, Ihre Mitarbeitenden befähigen und den Wert Ihrer Investition in Copilot für Microsoft 365 realisieren können. Weitere Beispiele nach Abteilung und Rolle finden sich unter den folgenden Links:



## Branchenspezifische Use Cases

In diesem Abschnitt werden die spezifischen Anwendungen von Copilot für Microsoft 365 in drei kritischen Branchen untersucht: Recht, Banken und Gesundheitswesen. Durch die Hervorhebung gezielter Use Cases demonstriert Microsoft die Effektivität von Copilot bei der Bewältigung branchenspezifischer Herausforderungen und der Verbesserung von Kernprozessen.

## Use Cases in der Rechtsbranche

+ **Vertragsüberprüfung und -analyse:** Automatisiert den Überprüfungsprozess durch den Vergleich von Vertragsklauseln mit rechtlichen Standards und früheren Verträgen. Dies erhöht die Effizienz, reduziert menschliche Fehler und gewährleistet die Einhaltung rechtlicher Standards.
+ **Unterstützung bei Rechtsstreitigkeiten:** hilft bei der Unternehmen und Analyse großer Mengen fallbezogener Daten zur Unterstützung von Rechtsstreitigkeiten. Dies spart Zeit und verbessert die Vorbereitung und Präsentation von rechtlichen Argumenten.
+ **Compliance Monitoring:** Es wird kontinuierlich nach Gesetzesänderungen gesucht, damit die Unternehmen alle relevanten Gesetze einhalten können. Dadurch wird das Risiko rechtlicher Sank-

tionen verringert und der Ruf des Unternehmens als sorgfältiges Unternehmen gestärkt.

## Use Cases im Bankensektor

+ **Betrugserkennung:** nutzt KI, um Transaktionen in Echtzeit zu überwachen und Muster zu erkennen, die auf betrügerische Aktivitäten hinweisen. Dies minimiert finanzielle Verluste und schützt das Vertrauen der Kunden.
+ **Risikobewertung:** Analyse von Kundendaten zur Vorhersage und Minderung potenzieller Risiken bei Krediten und Investitionen. Dadurch wird die Fähigkeit der Bank verbessert, Risiken wirksam zu steuern und zu mindern.
+ **Regulatory Compliance Tracking**: Verfolgt alle gesetzlichen Anforderungen und stellt sicher, dass die Bank die Finanzvorschriften einhält. Dadurch werden rechtliche Strafen vermieden und die betriebliche Integrität gewahrt.

## Use Cases im Gesundheitswesen

+ **Verwaltung von Patientendaten:** Verwaltung und Sicherung großer Mengen von Patientendaten, die den Gesundheitsdienstleistern einen einfachen Zugriff ermöglichen. Dies verbessert die Effizienz und Vertraulichkeit der Patientenversorgung.
+ **Diagnoseunterstützung:** Unterstützung bei der Diagnose von Krankheiten durch die Analyse von Patientendaten und medizinischem Bildmaterial. Dies erhöht die Genauigkeit der Diagnosen und die Wirksamkeit der Behandlungspläne.
+ **Fernüberwachung von Patienten:** Überwachung von Patienten aus der Ferne mit Hilfe von Daten aus tragbaren Geräten, die den Leistungserbringern Echtzeit-Updates zum Gesundheitszustand liefern. Dies verringert die Zahl der Wiederaufnahmen ins Krankenhaus und ermöglicht ein proaktives Gesundheitsmanagement.

# Anhang 2: Häufig gestellte Fragen (FAQs)

## Wie werden die Daten meines Unternehmens geschützt, wenn ich die Generative AI-Services von Microsoft verwende?

Microsoft lebt vom Vertrauen. Sie haben sich bei allem, was sie tun, der Sicherheit, dem Datenschutz und der Einhaltung von Vorschriften verschrieben, und der Ansatz für generative KI ist nicht anders.

Der Datenschutz ist Teil des Konzepts für verantwortungsvolle KI, und Microsoft wird bei seinen KI-Produkten und -Lösungen auch weiterhin die Grundwerte Datenschutz, Sicherheit, Fairness, Verantwortlichkeit, Transparenz, Zuverlässigkeit, Inklusion und Sicherheit hochhalten.

In Teil 2 dieses Papers werden sieben Verpflichtungen vorgestellt, die zeigen, dass Microsoft sich weiterhin für den Schutz der Daten der Kunden einsetzt, wenn sie generative KI-Dienste genutzt wird:

- Die Daten Ihrer Unternehmen werden von Microsoft vertraulich behandelt.
- Sie haben die Kontrolle über die Daten Ihres Unternehmens.
- Ihre Zugriffskontrolle und Unternehmensrichtlinien werden beibehalten.
- Die Daten Ihres Unternehmens werden nicht ohne Ihre Zustimmung weitergegeben.
- Der Datenschutz und die Datensicherheit Ihres Unternehmens sind durch das Design geschützt.
- Die Daten Ihres Unternehmens werden nicht ohne Ihre Zustimmung zum Trainieren von Foundation-Modellen verwendet.
- Unsere Produkte und Lösungen entsprechen weiterhin 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 erzeugen kann, die bereits bekannten Beispielen ähnlich sind. Sie tut dies, indem sie aus einer Reihe von Beispielen lernt, die Muster und Regeln herausfindet, die sie ähnlich machen, und dann diese Muster und Regeln verwendet, um neue Beispiele zu schaffen, die denen ähnlich sind, aus denen sie gelernt hat. Sie unterscheidet sich von anderen Arten der KI, weil sie neue Dinge erschaffen kann, anstatt nur Dinge zu erkennen oder zu klassifizieren, die sie bereits gesehen hat.

Microsofts Azure OpenAI-Dienst und Copilot für Microsoft 365 ermöglichen es Kunden, die OpenAI-Modelle, einschließlich GPT-3, GPT-4 und Codex, in der Microsoft-Umgebung zu nutzen. Diese Modelle werden gemeinhin als „Basismodelle“ bezeichnet. Darunter versteht man im Allgemeinen groß angelegte KI-Modelle, die in großem Umfang auf großen Mengen primär unbeschrifteter Daten trainiert werden (in der Regel durch selbstüberwachtes Lernen) und mit minimaler Feinabstimmung für eine Reihe verschiedener nachgelagerter Aufgaben angepasst werden können.

## Was sind die Unterschiede zwischen Cloud- und generativen KI-Diensten im Hinblick auf die DSGVO?

Für die Nutzung von Cloud-Computing-Diensten gelten dieselben Verpflichtungen wie für die Nutzung von generativen KI-Diensten gemäß der DSGVO. Die DSGVO verlangt einen risikobasierten Ansatz für die Implementierung und Nutzung aller neuen Technologien.

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

Erfahren Sie in Teil 2 dieses Papers mehr darüber, wie Microsoft Kunden bei der Durchführung dieser Bewertung unterstützen kann, wenn sie Copilot für Microsoft 365 und / oder Azure OpenAI Service nutzen möchten.

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

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

Zu den wichtigsten Verpflichtungen, die Unternehmen bei der Beschaffung und / oder Implementierung von generativen KI-Systemen berücksichtigen sollten, gehören:

- prüfen, ob Sie Ihre Datenschutzhinweise aktualisieren müssen, um neue Verarbeitungstätigkeiten widerzuspiegeln oder Tätigkeiten zu verdeutlichen (Artikel 12 - 14);
- sicherstellen, dass Sie über Verfahren verfügen, die es Ihnen ermöglichen, Anfragen zu den Rechten der betroffenen Personen nachzukommen (Artikel 15 - 21 der DSGVO);
- sicherstellen, dass jede Vereinbarung, die Sie mit einem Datenverarbeiter treffen, mit Artikel 28 der DSGVO übereinstimmt, auch in Bezug auf Sicherheitsmaßnahmen und internationale Übermittlungen;
- zu prüfen, ob Sie eine Datenschutz-Folgenabschätzung (DPIA) durchführen müssen (Artikel 35 der DSGVO); und
- sicherstellen, dass alle Datenübermittlungen außerhalb des Vereinigten Königreichs, der EU oder des EWR im Rahmen eines gültigen Übermittlungsverfahrens erfolgen (Artikel 44-50).

Erfahren Sie in Teil 2 des Papers mehr darüber, wie Microsoft seine Kunden bei der Erfüllung dieser Verpflichtungen unterstützt.

## Wie interagiert die DSGVO mit dem KI-Gesetz?

Das KI-Gesetz ist ein neues Gesetz, das derzeit in der EU eingeführt wird, um KI-Systeme zu regulieren. Es wird für Anbieter, Importeure, Vertreiber, Nutzer und andere am KI-Lebenszyklus Beteiligte gelten und soll sicherstellen, dass KI-Systeme, die in der EU eingesetzt werden, die Grundrechte, die Sicherheit und ethische Grundsätze einhalten und bestimmte Risiken im Zusammenhang mit den leistungsfähigsten KI-Modellen für allgemeine Zwecke angehen.

Die DSGVO und das KI-Gesetz sollen sich gegenseitig ergänzen und einen Rechtsrahmen für KI- Produkte und -Dienste schaffen.

Die DSGVO, die die Verarbeitung personenbezogener Daten durch die für die Datenverarbeitung Verantwortlichen und die Datenverarbeiter regelt, konzentriert sich auf den Datenschutz und zielt darauf ab, dem Einzelnen die Kontrolle über seine personenbezogenen Daten zu geben. Im Rahmen des KI-Gesetzes wird der GroßTeil der regulatorischen Belastung auf Anbieter von KI-Systemen mit hohem Risiko und von KI-Modellen für allgemeine Zwecke (GPAI) entfallen.

Obwohl sich die DSGVO und das Gesetz über künstliche Intelligenz in Bezug auf ihren Anwendungsbereich und ihren Zweck unterscheiden, stehen sie in mehrfacher Hinsicht in Wechselwirkung zueinander.

Zum Beispiel:

+ Die DSGVO verpflichtet die für die Datenverarbeitung Verantwortlichen, unter bestimmten Umständen eine Datenschutzfolgenabschätzung durchzuführen. Das KI-Gesetz verweist auf diese Verpflichtung und verlangt von den Nutzern von KI-Systemen mit hohem Risiko, bestimmte obligatorische nutzerbezogene Informationen zu verwenden, um ihren DPIA-Verpflichtungen gemäß der DSGVO nachzukommen.
+ Die DSGVO gilt, wenn personenbezogene Daten verarbeitet werden, um ein KI-System zu trainieren, oder wenn ein KI- System verwendet wird, um personenbezogene Daten zu verarbeiten.

Die Annahme der in diesem Paper beschriebenen Maßnahmen zur Einhaltung der DSGVO ergänzt daher das Gesetz über künstliche Intelligenz und die damit verbundenen Verpflichtungen, die im Rahmen dieser neuen Gesetzgebung gelten werden.

Microsoft hat sich zur Einhaltung des EU-KI-Gesetzes verpflichtet. Microsofts mehrjährige Bemühungen, den Microsoft Responsible AI Standard zu definieren, weiterzuentwickeln und zu implementieren, sowie die interne Governance haben ihre Einsatzbereitschaft erhöht. Sobald die endgültigen Anforderungen im Rahmen des EU-KI-Gesetzes genauer definiert sind, freut sich auf die Zusammenarbeit mit den politischen Entscheidungsträgern, um eine praktikable Umsetzung und Anwendung der Vorschriften sicherzustellen, die Konformität nachzuweisen und mit den Kunden und anderen Stakeholdern zusammenzuarbeiten, um die Einhaltung der Vorschriften im gesamten Ökosystem zu unterstützen.

## Wie hält Microsoft das geltende Recht ein?

Die KI-Produkte und -Lösungen von Microsoft sind so konzipiert und aufgebaut, dass sie die geltenden Datenschutzgesetze, einschließlich DSGVO, einhalten.

Microsofts Ansatz zum Schutz der Privatsphäre in der KI wird durch die Verpflichtung zur Einhaltung bestehender und neu entstehender regulatorischer und rechtlicher Verpflichtungen auf der ganzen Welt untermauert. Microsoft wird sich weiterhin für eine sinnvolle Regulierung des Datenschutzes und der KI einsetzen und sind der Meinung, dass der beste Weg zu raschen Fortschritten bei den erforderlichen Leitplanken für KI darin besteht, sich auf bestehende rechtliche Schutzmaßnahmen, Ansätze und Regulierungsinstrumente zu stützen, die bereits heute auf den Schutz der Privatsphäre und die Sicherheit dieser Systeme angewendet werden könnten.

## Teilt Microsoft Kundendaten mit OpenAI / ChatGPT?

Nein. Die Kundendaten Ihres Unternehmens, einschließlich Prompts (Inputs) und Vervollständigungen (Outputs), Ihre Einbettungen und alle Trainingsdaten, die Sie den Microsoft Online Services zur Verfügung stellen, sind für OpenAI nicht verfügbar.

Der Azure OpenAI Service wird vollständig von Microsoft kontrolliert; Microsoft hostet die OpenAI-Modelle in Microsofts Azure-Umgebung und der Azure OpenAI Service interagiert nicht mit den von OpenAI betriebenen Diensten (z. B. ChatGPT oder die OpenAI API). OpenAI ist kein Unterprozessor von Microsoft

> Mehr Informationen über die zugrunde liegenden OpenAI-Modelle, die den Azure OpenAI Service antreiben

## Kann ich vertrauliche Informationen mit den generativen KI-Diensten von Microsoft teilen?

Ja. Bei der Nutzung von Azure OpenAI oder Copilot für Microsoft 365 können Kunden ihre vertraulichen Informationen vertrauensvoll weitergeben. Die Basismodelle, auf die über Azure OpenAI Service und Copilot für Microsoft 365 zugegriffen wird, verwenden keine Kundendaten für Schulungen ohne Erlaubnis. Diese Basismodelle sind zustandslos und speichern keine Daten, einschließlich der Prompts, die ein Kunde eingibt, und der Vervollständigungen, die das Modell ausgibt. Die Kunden können auch darauf vertrauen, dass ihre vertraulichen Informationen nicht an andere Kunden weitergegeben werden.

## Wie schützt Microsoft die Sicherheit in dieser neuen Ära der KI?

Die Sicherheit ist in den gesamten Entwicklungszyklus aller Microsoft-Unternehmensdienste (einschließlich derjenigen, die generative KI-Technologie enthalten) integriert, von der Konzeption bis zur Bereitstellung.

Azure OpenAI Service und Copilot für Microsoft 365 werden 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 Vorteile der Sicherheits- und Compliance-Funktionen zu nutzen, die in Microsofts Hyperscale-Cloud bereits gut etabliert sind.

Dazu gehört die Priorisierung von Zuverlässigkeit, Redundanz, Verfügbarkeit und Skalierbarkeit, die alle standardmäßig in Microsoft Cloud-Services integriert sind.

Da es sich bei generativen KI-Systemen auch um Softwaresysteme handelt, kommen alle Elemente des Sicherheitsentwicklungszyklus zur Anwendung: von der Bedrohungsmodellierung über die statische Analyse, die sichere Erstellung und den sicheren Betrieb bis hin zur Verwendung starker Kryptografie, Identitätsstandards und mehr.

Microsoft hat auch neue Schritte zu seinem Security Development Lifecycle hinzugefügt, um sich auf KI- Bedrohungsvektoren vorzubereiten, einschließlich der Aktualisierung der SDL-Anforderung zur Bedrohungsmodellierung, um KI- und Machine-Learning-spezifische Bedrohungen zu berücksichtigen. Microsoft hat seine KI-Produkte einem KI-Red-Teaming unterzogen, um nach Schwachstellen zu suchen und sicherzustellen, dass sie über geeignete Strategien zur Risikominderung verfügen.

Mehr Informationen über Sicherheit für Copilot für Microsoft 365 in Teil 3 dieses Papers und über Sicherheit für Azure OpenAI Service in Teil 4 dieses Papers.

## Sind Datenübermittlungen in Länder ausserhalb des Vereinigten Königreichs, der EU oder des EWR nach der DSGVO zulässig?

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

Bei der Übermittlung personenbezogener Daten durch Microsoft außerhalb des Vereinigten Königreichs, der EU oder des EWR kommen gültige Übermittlungsmechanismen im Rahmen der DSGVO zum Einsatz, einschließlich der EU-U.S. Data Privacy Framework-Zertifizierung und der EU-Standardvertragsklauseln.

In Teil 2 dieses Dokuments erfahren Sie mehr darüber, wie Microsoft die Datenübermittlung an Drittländer handhabt.

## Wo werden meine Daten gespeichert und verarbeitet?

Die Wahl der Datenresidenz wird respektiert, wenn Sie Produkte und Dienste der generativen KI von Microsoft nutzen, die lokale Speicher- und / oder Verarbeitungsfunktionen bieten.

Azure OpenAI Service und Copilot für Microsoft 365 verarbeiten und speichern Ihre Daten innerhalb der EU / EFTA für EU Data Boundary (EUDB) Kunden, wie in den Produktbedingungen und der EU Data Boundary Transparency Documentation dargelegt.

## Müssen Unternehmen einen individuellen Datenschutzzusatz (DPA) entwickeln?

Nein, die DSGVO schreibt nicht vor, dass jeder für die Verarbeitung Verantwortliche ein individuelles Datenschutzzusatz (DPA) mit seinen Datenverarbeitern abschließt. Das Datenschutzzusatz (DPA)von Microsoft entspricht den Anforderungen von Artikel 28 der DSGVO.

Es ist für Hyperscale-Cloud-Anbieter nicht praktikabel, unterschiedliche Bedingungen für verschiedene Kunden anzubieten, da es die Einheitlichkeit der Dienste ist, die Cloud-Dienste verwaltbarer, skalierbarer, sicherer und erschwinglicher macht als Lösungen vor Ort. Darüber hinaus könnte die Einführung unterschiedlicher Sicherheitsmaßnahmen oder -standards für verschiedene Kunden die Sicherheit der Microsoft-Dienste insgesamt untergraben. Daher ist es für Microsoft nicht machbar, seine betrieblichen Abläufe zu ändern oder für jeden Kunden maßgeschneiderte vertragliche Verpflichtungen und / oder eine eigene Vertragsstruktur zu schaffen.

Mehr Informationen über Microsofts Pflichten als Datenverarbeiter Verpflichtungen in Teil 2 dieses Papers.

## Wie können Kunden ihre Nutzung generativer KI-Dienste 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, vom ersten Entwurf bis zur endgültigen Umsetzung.

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

Eine Möglichkeit, die Einhaltung d e r DSGVO nachzuweisen, ist die Durchführung einer Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) für bestimmte Use Cases von generativen KI-Lösungen. Eine Datenschutz-Folgenabschätzung hilft Unternehmenen, Datenschutzrisiken zu identifizieren und zu reduzieren. Eine Datenschutz-Folgenabschätzung ist gesetzlich vorgeschrieben, wenn die Verarbeitungstätigkeit wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Auch wenn sie nicht gesetzlich vorgeschrieben ist, ist eine Datenschutzfolgenabschätzung eine gute Praxis und kann Ihnen dabei helfen, die spezifischen Datenschutzrisiken im Zusammenhang mit der Art und Weise, wie Sie generative KI für einen bestimmten Use Case implementieren möchten, zu ermitteln.

In Teil 2 dieses Papers erfahren Sie mehr über Datenschutzfolgenabschätzungen.

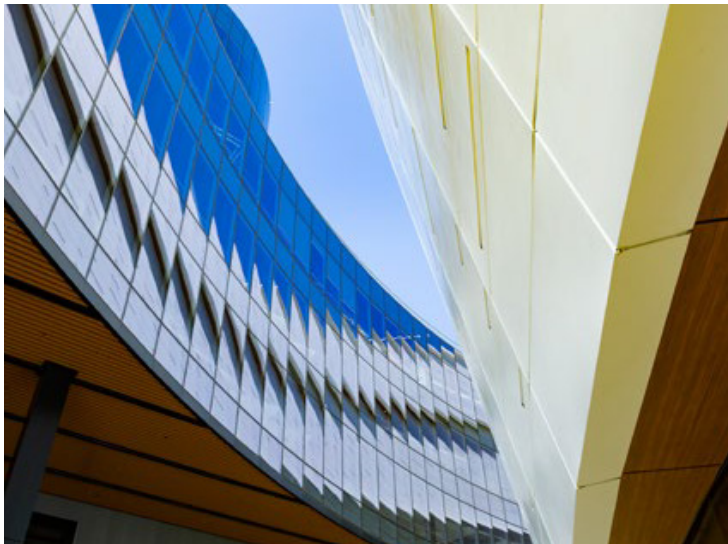
## Können Kunden die DSGVO einhalten, wenn sie eine öffentliche Cloud für die Nutzung generativer KI-Dienste nutzen?

Die öffentlichen Cloud-Dienste von Microsoft wurden entwickelt, um sicherzustellen, dass sie von den Kunden in Übereinstimmung mit der DSGVO genutzt werden können (und viele Kunden nutzen diese Dienste bereits). Die in diesem Paper dargelegten und in den Produktbedingungen und den Datenschutzzusatz (DPA) enthaltenen Informationen können von Ihnen verwendet werden, um eine angemessene risikobasierte Bewertung der vorgeschlagenen Nutzung von Copilot für Microsoft 365 und Azure OpenAI Service vorzunehmen, u m die Einhaltung der einschlägigen Anforderungen der DSGVO nachzuweisen.

## Wie können Unternehmen ihre Transparenz^-verpflichtungen im Rahmen der DSGVO beim Einsatz von KI- Technologien erfüllen ?

Nach den Artikeln 12 bis 14 der DSGVO sind Unternehmen verpflichtet, den betroffenen Personen bestimmte Schlüsselinformationen über die Verwendung ihrer personenbezogenen Daten zur Verfügung zu stellen. Diese Informationen werden häufig in Form von Datenschutzhinweisen bereitgestellt. Wenn Sie eine neue Technologie einsetzen (z. B. Copilot für Microsoft 365 oder Azure OpenAI Service) und beabsichtigen, diese Technologie auf eine Weise zu nutzen, die nicht in Ihren bisherigen Datenschutzhinweisen enthalten ist, müssen Sie deren Datenschutzhinweise aktualisieren, um diese neuen Verarbeitungstätigkeiten widerzuspiegeln.

Die in diesem Dokument enthaltenen Informationen sollen helfen zu verstehen, wie Copilot für Microsoft 365 und Azure OpenAI Service Daten verwenden und welche Informationen den betroffenen Personen mitgeteilt werden müssen.



# Anhang 3: Zusätzliche Ressourcen

Microsoft ist bestrebt, seinen Kunden klare Informationen darüber zu geben, wie Daten verwendt und weitergeben werden und welche Möglichkeiten sie bei der Verwaltung ihrer Daten haben. In diesem Anhang finden sich zusätzliche Ressourcen, die Sie zur Ergänzung und Vertiefung der in diesem Dokument dargelegten Informationen nutzen können.

### Responsible AI

- Empowering responsible AI practices
- Governing AI: A Blueprint for the Future
- Microsoft's principles and approach to Responsible AI
- Microsoft Responsible AI Standard
- Responsible AI Transparency Report

### Microsoft's Customer Commitments

- AI Assurance Program and AI Customer Commitments
- Customer Copyright Commitment
- 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

### Understanding Generative AI

- The underlying LLMs that power Microsoft's generative AI solutions
- The art and science of prompting (the ingredients of a prompt)
- Prompting do's and don'ts

### Data Protection Addendum and Product Terms

- Data Protection Addendum
- Microsoft Product Terms

### Data Residency Commitments

- The EU Data Boundary
- EU Data Boundary Transparency Documentation
- Advanced Data Residency (ADR)
- Multi-Geo Capabilities

### Data Protection Impact Assessments (DPIA)

- DPIAs and their contents
- Data Protection Impact Assessments for the GDPR

### AI for Business

- AI Solutions for Organizations
- AI driven businesses surge ahead of competition
- AI business value and benefits
- The business opportunity of AI

### Copilot for Microsoft 365

- Copilot for Microsoft 365
- Copilot Lab
- Copilot for Microsoft 365 Documentation
- Data, Privacy, and Security for Copilot for Microsoft 365
- FAQs for Copilot data security and privacy
- Microsoft 365 isolation controls
- Encryption in the Microsoft Cloud
- Microsoft Copilot Scenario Library

### Azure OpenAI Service

- Azure OpenAI Service - Documentation, quickstarts and API reference guides
- Configure usage rights for Azure Information Protection
- Data, privacy and security for Azure OpenAI Service
- Prompt Engineering
- Azure OpenAI On Your Data
- Azure OpenAI fine tuning
- Content filtering
- Abuse monitoring
- Enterprise security for Azure Machine Learning