

# Datenschutz in der Kanzlei - Microsoft 365 und Lösungen im Bereich Künstliche Intelligenz

# Welche Rolle spielt Datenschutz in Bezug auf M365?

- Datenschutz spielt eine äußerst wichtige Rolle in Bezug auf Microsoft 365 (früher Office 365). Da Microsoft 365 eine umfassende Plattform für Kommunikation, Zusammenarbeit und Datenspeicherung ist, beinhaltet sie viele persönliche und geschäftliche Daten. Hier sind einige Schlüsselaspekte, die den Datenschutz in Bezug auf Microsoft 365 betreffen.

Datenverarbeitung und -speicherung: Microsoft 365 speichert und verarbeitet verschiedene Arten von Daten, darunter E-Mails, Dokumente, Kalendereinträge und mehr. Es ist wichtig zu verstehen, wie diese Daten erfasst, gespeichert und verarbeitet werden, um sicherzustellen, dass der Datenschutz gewährleistet ist.

- Der Datenschutz in Bezug auf Microsoft 365 ist ein kontinuierlicher Prozess, der sorgfältige Planung, Umsetzung und Überwachung erfordert, um sicherzustellen, dass die persönlichen und geschäftlichen Daten angemessen geschützt werden.

# Wie können Sie Microsoft 365 datenschutzkonform nutzen?

- Finden Sie die optimale Lizenzierung für die Bedürfnisse Ihres Unternehmens
- Stellen Sie sicher, dass alle notwendigen Verträge vorliegen
- Beziehen Sie den Betriebsrat mit ein (falls vorhanden)
- Konfiguration Ihres Microsoft 365 Tenants und Anpassung Ihrer Sicherheitseinstellungen
- Anfertigung einer Risikoanalyse
- Verzeichnis von Verarbeitungstätigkeiten
- Erstellen eines Berechtigungskonzept
- Binden Sie Ihre Mitarbeiter ein
- Administratoren und Datenschutz
- Implementierung eines Dokumentenmanagementsystem (DMS)

# Beispielfragen zu Microsoft 365

- 1.1 Können Sie erläutern, welche Lizenzen und Services für Ihren Microsoft Tenant aktuell aktiviert sind?
- 1.2 Liegen Ihnen die Organisationsdaten vor, die für Ihren Microsoft Tenant hinterlegt sind?
- 1.3 Nutzen Sie die Customer Lockbox-Funktion um den Zugriff auf Ihre Daten durch Microsoft-Mitarbeiter zu verhindern?
- 1.4 Nutzen Sie die Customer Keys Funktion bei Microsoft Services?
- 1.5 Liegt Ihnen der Microsoft\_Customer\_Agreement vor?
- 1.6 Liegt Ihnen der Microsoft Products and Services Data Protection Addendum (DPA) vor?
- 1.7 Liegt Ihnen der Service Level Agreements (SLA) for Online Services vor?
- 1.8 Liegt Ihnen das EU-U.S. Data Privacy Framework Abkommen vor?
- 1.9 Liegt Ihnen eine Dienstvereinbarung (nur wenn Betriebsrat vorhanden) vor?
- 2.1 Multi-Faktor-Authentifizierung (MFA): Haben Sie MFA für alle Benutzerkonten aktiviert, um die Sicherheit zu erhöhen?
- 2.2 Rollenbasierte Zugriffskontrolle (RBAC): Stellen Sie sicher, dass Benutzer nur Zugriff auf die für ihre Arbeit notwendigen Informationen und Funktionen haben?
- 2.3 Datenschutz und Compliance-Einstellungen: Sind Sie den "Microsoft Compliance Manager" durchgegangen und sind sie den Empfehlungen nachgekommen?
- 2.4 Haben Sie Microsoft Defender for Identity (ehemals ATP), Anti-Phishing, Anti-Spam und Anti-Malware in Ihrem Microsoft Tenant aktiviert, um Ihre E-Mail-Kommunikation zu sichern?
- 2.5 Sind in Ihrem Microsoft Tenant Audit-Logs aktiviert, um Aktivitäten innerhalb Ihres Tenants überwachen zu können?
- 2.6 Nutzen Sie Microsoft Intune (Endpoint Manager) für die Verwaltung von Geräten und die Anwendung von Sicherheitsrichtlinien auf Geräte, die auf Unternehmensdaten zugreifen?
- 2.7 Haben Sie die Einstellungen für SharePoint und OneDrive in Ihrem Unternehmen konfiguriert, um sicherzustellen, dass Dateien sicher gespeichert und nur mit autorisierten Personen geteilt werden?
- 2.8 Implementieren Sie in Ihrem Unternehmen strenge Passwortrichtlinien und ermutigen Sie Benutzer, ihre Passwörter regelmäßig zu ändern?
- 2.9 Stellen Sie sicher, dass alle Benutzer in Ihrem Unternehmen in Bezug auf Cybersicherheit und Datenschutz geschult sind?
- 2.10 Telemetrie und Diagnosedaten: Überprüfen Sie, ob die Telemetrie-Daten und Diagnosedaten in Ihrem Microsoft 365 Tenant datenschutzkonform konfiguriert sind, um sowohl die Leistung und Sicherheit Ihrer Umgebung zu gewährleisten als auch die Datenschutzrichtlinien und Compliance-Anforderungen Ihres Unternehmens zu erfüllen.

- Künstliche Intelligenz (KI) gewinnt in Steuerkanzleien zunehmend an Bedeutung, da sie die Effizienz und Genauigkeit bei der Bearbeitung von Steuer- und Finanzprozessen erheblich steigern kann. Angesichts steigender Anforderungen durch gesetzliche Vorschriften, komplexe Datenmengen und den Bedarf an zeitnahen Auswertungen wird KI zu einem unverzichtbaren Werkzeug.

# Vorteile von KI für Steuerkanzleien:

- **Automatisierung von Routineaufgaben:** KI kann zeitintensive Tätigkeiten wie das Verarbeiten von Belegen, das Kategorisieren von Transaktionen oder das Erstellen von Buchungsjournalen übernehmen.
- **Verbesserung der Datenanalyse:** Mit KI können Kanzleien große Datenmengen analysieren, Anomalien erkennen und präzisere Vorhersagen für Steuerplanung und Liquiditätsmanagement treffen.
- **Fehlerreduktion:** Durch maschinelles Lernen werden Eingabefehler minimiert, was die Qualität der Daten und der daraus resultierenden Analysen verbessert.
- **Zeit- und Kostenersparnis:** Automatisierte Prozesse sparen nicht nur Arbeitszeit, sondern ermöglichen es den Steuerberatern, sich auf komplexere Mandantenfragen zu konzentrieren.

- Die DATEV eG hat die Bedeutung von KI für die Steuerberatung bereits erkannt und integriert diese Technologie aktiv in ihre Produkte. Auf ihrer Website weist DATEV darauf hin, dass „**einige KI-basierte Produkte bereits verfügbar**“ sind. Diese Anwendungen nutzen KI, um Arbeitsprozesse zu vereinfachen, z. B. durch die automatische Texterkennung oder die intelligente Erfassung und Verarbeitung von Belegen.
- DATEV setzt damit nicht nur auf moderne Technologien, sondern bietet Steuerkanzleien konkrete Werkzeuge, um im Wettbewerb konkurrenzfähig zu bleiben. Kanzleien, die solche Technologien einsetzen, profitieren von optimierten Prozessen und können sich als innovativ und zukunftsorientiert positionieren.
- Einige KI-basierte Produkte sind bereits bei der DATEV verfügbar  
<https://www.datev.de/web/de/ueber-datev/datev-und-ki/#:~:text=Einige%20KI%2Dbasierte%20Produkte%20sind%20bereits%20verf%C3%BCgbar%3A>

# Warum Microsoft Copilot eine Wahl sein kann?

1. Bessere Integration in bestehende Datenschutzmaßnahmen
2. Kontrolle über die Datenverarbeitung
3. Sicherheitsfunktionen und Compliance
4. Datenverarbeitung durch Drittanbieter



# 10 einfache Prompt Beispiele für CoPilot

- **1. E-Mail schreiben:** "Schreibe eine E-Mail an das Team, um das nächste Meeting zu planen."
- **2. Termin erstellen:** "Erstelle einen Kalendereintrag für das wöchentliche Team-Meeting am Freitag um 10 Uhr."
- **3. Aufgabenliste erstellen:** "Erstelle eine To-Do-Liste für die Aufgaben, die heute erledigt werden müssen."
- **4. Dokument zusammenfassen:** "Fasse das Dokument Projektplan in wenigen Sätzen zusammen."
- **5. Erinnerung setzen:** "Setze eine Erinnerung für den Abgabetermin des Berichts am Montag."
- **6. Notizen machen:** "Erstelle Notizen für das Meeting mit dem Kunden am Mittwoch."
- **7. Bericht erstellen:** "Erstelle einen wöchentlichen Fortschrittsbericht für das Projekt."
- **8. Datei suchen:** "Finde die neueste Version der Präsentation für das Projekt."
- **9. Kontaktinformationen finden:** "Finde die Kontaktinformationen von DATA Security."
- **10. Feedback einholen:** "Schicke eine Umfrage an das Team, um Feedback zum letzten Meeting zu erhalten."

# Was gilt es bei der Verwendung von Daten in Online-KI-Anwendungen grundlegend zu beachten?

- Online-KI-Werkzeuge wie ChatGPT, Microsoft Copilot oder auch Übersetzungsprogramme wie Google Translator oder DeepL können Sie bei Ihren Aufgaben unterstützen. Beim Umgang mit den KI-Produkten gibt es aber diverse Fallstricke, die Sie bei der Nutzung dieser Programme beachten müssen. Diese können die Nutzung dann auch einschränken.
- Wichtig ist, dass Sie klar definieren, für welche Zwecke die KI eingesetzt werden darf. Durch verantwortungsloses oder unbedarftes Handeln können durchaus Haftungsfragen auf Grund von Gesetzesverstößen oder durch Verletzungen des Urheberrechts entstehen.

- Verwenden Sie keine personenbezogenen Daten (das sind alle Angaben, die Rückschlüsse auf eine bestimmbare oder bestimmte natürliche Person zulassen)
- Machen Sie keine Angaben zu besonders schützenswerten Personendaten. Hierrunter fallen Angaben zu religiösen, weltanschaulichen und politischen Ansichten und Tätigkeiten. Außerdem auch biometrische Daten, durch die eine natürliche Person eindeutig bestimmt werden kann. Auch Daten zur Intimsphäre, ethnischen Zugehörigkeit oder Gesundheit fallen hier drunter. Des Weiteren alle Angaben zu Maßnahmen sozialer Hilfe sowie zu strafrechtlichen oder disziplinarischen Verfahren oder Sanktionen
- Erstellen Sie keine Persönlichkeitsprofile und betreiben Sie auch kein Profiling.

# KI und Geheimhaltungsverpflichtungen

- Machen Sie keine Angaben zu vertraglich ausdrücklich geschützten Daten.
- Machen Sie keine Angaben, wenn diese besonderen Geheimnissen unterliegen (Berufsgeheimnis wie Arztgeheimnis, Steuergeheimnis, Betriebsgeheimnis, Amtsgeheimnis, etc.)

- Die Hersteller der KI-Anwendungen sind in der Regel nicht für die Inhalte verantwortlich!
- Seien Sie sich deshalb bewusst, dass der in der KI generierte Text aus diversen Quellen stammt. Es liegt in der Verantwortung des Nutzers zu prüfen, ob der Text oder ob Textpassagen urheberrechtlich geschützt sind!
- Alle erwähnten Punkte sind auch bei der Verwendung von Bildern, privaten Fotos, Tonaufnahmen, Videos, Simulationen oder Codes in Online-KI-Anwendungen zu beachten!

# Fazit: Datenschutz in der Kanzlei – Microsoft 365 und KI-Lösungen

Der Einsatz von Microsoft 365 und KI-Lösungen in der Kanzlei mag bei Skeptikern Bedenken hervorrufen, insbesondere in Bezug auf Datenschutz und Sicherheit. Doch eines ist klar: Die Digitalisierung wird nicht nur weiter voranschreiten, sie wird zunehmend unverzichtbar. Der Schlüssel liegt darin, sich gut vorbereitet auf diese Zukunft einzulassen.

Moderne Lösungen wie KI-gestützte Automatisierung bieten bereits heute erhebliche Arbeitserleichterungen. Routinetätigkeiten werden schneller und präziser erledigt, was wertvolle Zeit für komplexere, beratungsintensive Aufgaben freisetzt – genau dort, wo menschliche Expertise gefragt ist. Wer sich frühzeitig mit den Technologien vertraut macht und auf datenschutzkonforme Implementierungen achtet, profitiert doppelt: durch Effizienzgewinne im Hier und Jetzt und durch die Gewissheit, auch morgen technologisch und rechtlich auf der sicheren Seite zu sein.