Ein Schwerpunkt für die Privation, die Sekurität und die Best Praktiken

AI IN DER BUCHHALTUNG

Europäischer Verband der Buchhalter und Wirtschaftsprüfer für KMU

+32 (0)2 736 88 86 | secretariat@efaa.com | www.efaa.com

AI im Rechnungswesen: Eine Einführung

Die KI revolutioniert den Beruf des Buchhalters völlig. Aktuelle Anwendungen können routinemäßige Buchhaltungsaufgaben wie Buchführung, Rechnungsprüfung und Datenanalyse automatisieren, wodurch KMU Zeit gewinnen, um ihren Kunden zusätzliche Dienstleistungen anzubieten und sich auf strategische Aktivitäten zu konzentrieren. Diese Automatisierungen können auch menschliche Fehler reduzieren.

Trotz ihrer vielen Vorteile birgt die Integration von KI in die Buchhaltung auch potenzielle Risiken. Dazu gehören vor allem Bedenken hinsichtlich der Datensicherheit und des Datenschutzes.

Die Buchhaltungsbranche befindet sich an einem kritischen Punkt, an dem die Unternehmen ein Gleichgewicht zwischen Innovation und Vorsicht finden müssen. Immer mehr fortschrittliche Tools werden in die Buchhaltungssysteme integriert. Dennoch müssen Buchhaltungsexperten wachsam bleiben, um die Datenintegrität zu wahren, die Einhaltung von Vorschriften zu gewährleisten und die menschliche Kontrolle zu erhalten.

Dies ist der erste Leitfaden der EFAA zum Einsatz von KI im Rechnungswesen, der sich auf Sicherheits- und Datenschutzaspekte konzentriert. Weitere Ausgaben zu anderen KI-Themen sind für die Zukunft vorgesehen.

Datenschutz in AI-gesteuerten Buchhaltungssystemen

Beim Einsatz von KI in der Buchhaltung handelt es sich bei sensiblen Daten nicht nur um Finanzdaten wie Bilanzen und Cashflow-Aufzeichnungen, sondern auch um personenbezogene Daten von Kunden, Mitarbeitern und Lieferanten. KI-Lösungen verarbeiten diese Informationen durch ausgeklügelte Algorithmen, die Muster analysieren, Ergebnisse vorhersagen und Routineaufgaben in der Buchhaltung automatisieren.

Die Speicher- und Verarbeitungsmechanismen der KI-Tools unterscheiden sich erheblich. Viele arbeiten mit Cloud-basierten Infrastrukturen, bei denen die Daten über mehrere Server und Gerichtsbarkeiten verteilt sein können. Kostenlose und weit verbreitete Tools können durchaus Kundendaten für das Modelltraining verwenden und damit möglicherweise sensible Informationen preisgeben. Für Unternehmen ist es wichtig zu verstehen, dass es bei der Datensicherheit nicht nur darum geht, direkte Verstöße zu verhindern, sondern auch zu kontrollieren, wie Informationen durch das KI-Ökosystem fließen, einschließlich APIs, temporärer Speicherung und Verarbeitungsvereinbarungen mit Dritten.

EU Artificial Intelligence Act

Was ist das AI-Gesetz?

Neben der Datenschutz-Grundverordnung hat die EU eine weitere wichtige Rechtsvorschrift erlassen, die erhebliche Auswirkungen auf Unternehmen hat, die KI für Buchhaltungszwecke einsetzen.

Das KI-Gesetz reguliert KI-Technologien auf der Grundlage von Risikostufen. Für Wirtschaftsprüfungsunternehmen bedeutet dies, dass KI-Tools, die zur Finanzanalyse, Betrugserkennung oder Kreditwürdigkeitsprüfung eingesetzt werden, möglicherweise einer strengeren Prüfung und Compliance-Anforderungen unterliegen.

"Wir dürfen keine Zeit mit der Verabschiedung von Vorschriften zur Kontrolle des Einsatzes von KI verlieren.

- Margrethe Vestager, Exekutiv-Vizepräsidentin der Europäischen Kommission

Auswahl von sicheren AI-Anbietern für die Buchhaltung

Bei der Auswahl von KI-Tools für Rechnungswesen sollten die Sicherheitsmerkmale eine wichtige spielen. SMPs sollten Tools bevorzugen, die angemessene Sicherheitsmaßnahmen bieten, einschließlich Ende-zu-Ende-Verschlüsselung, sichere APIs für die Datenübertragung und umfassende Zugangskontrollen.
Unternehmenslösungen bieten in der Regel bessere und strengere Sicherheitsfunktionen als kostenlose, verbraucherorientierte Alternativen. Die "kostenlosen" KI-Tools sind mit Vorsicht zu genießen, da sie häufig auf Geschäftsmodellen beruhen, bei denen die Nutzerdaten zum Produkt werden.

Sie können die eingegebenen Daten auch für Schulungszwecke aufbewahren. KMPs sollten gründliche Anbieterbewertungen durchführen, die die Überprüfung von Sicherheitszertifizierungen (z. B. SOC 2), das Verständnis von Richtlinien zur Datenaufbewahrung und die Prüfung der Compliance-Historie des Anbieters umfassen.
KMUs sollten KI-Funktionen in Betracht ziehen, die in etablierte Softwareplattformen integriert sind (z. B. Co-Pilot in Sage), da diese in der Regel innerhalb eines für Finanzdaten konzipierten Sicherheitsrahmens arbeiten.

Bewährte Praktiken zum Schutz von Kundendaten

Eine der wichtigsten Strategien, die SMPs anwenden können, sind Techniken zur Anonymisierung und Maskierung von Daten. Durch das Entfernen (oder Verschlüsseln) persönlich identifizierbarer Informationen, bevor sie in KI-Systeme gelangen, kann das Risiko der Offenlegung sensibler Kundendaten drastisch reduziert werden.

Dieser Prozess kann teilweise durch KI-Tools automatisiert werden, die sensible Informationen aus Finanzdokumenten identifizieren und vor der Analyse unkenntlich machen. Es liegt auf der Hand, dass verschiedene Ebenen der Anonymisierung von Daten für unterschiedliche Zwecke geeignet sein können - von der vollständigen Anonymisierung für allgemeine Musteranalysen bis hin zur Pseudonymisierung für Arbeitsabläufe, bei denen eine gewisse Fähigkeit zur Re-Identifizierung erhalten bleiben muss. Es gibt auch fortgeschrittene Techniken (wie z. . differentieller Datenschutz), die implementiert werden könnten, um Datensätze mit statistischem "Rauschen" zu versehen, während ihr analytischer Wert erhalten bleibt.

Verschlüsselung ist eine grundlegende Schutzkomponente, wenn es um Buchhaltungsdaten in KI-Systemen geht. Die Unternehmen sollten für alle Kundendaten eine Verschlüsselung in Bankqualität (AES-256 oder höher) einsetzen und sicherstellen, dass die Verschlüsselungsschlüssel sicher verwaltet werden. Wenn Daten zwischen Buchhaltungssoftware und KI-Analysetools ausgetauscht werden, sollten sichere API-Verbindungen (mit TLS 1.3 oder gleichwertigen Protokollen) obligatorisch sein. Generell wird durch die Implementierung strenger rollenbasierter Zugriffskontrollen sichergestellt, dass nur befugtes Personal auf bestimmte Arten von Kundendaten zugreifen kann.

Eine proaktive Strategie zum Schutz der Kundendaten sollte regelmäßige Sicherheitsbewertungen und eine kontinuierliche Überwachung umfassen. Eine KI-gesteuerte Sicherheitsüberwachung kann ungewöhnliche Datenzugriffsmuster oder potenzielle Verstöße in Echtzeit erkennen. Darüber hinaus sollten Unternehmen vollständige Prüfprotokolle aller KI-Interaktionen mit Kundendaten führen.

Implementierung einer sicheren KI-Nutzung in Ihrem Unternehmen

Wie man eine umfassende KI-Politik entwickelt:

- Eindeutig festlegen, welche KI-Tools zur Verwendung zugelassen sind.
- Legen Sie die Arten von Daten fest, die in sie eingegeben werden können.
- Unterscheidung zwischen dem Umgang mit vertraulichen und nicht vertraulichen Informationen.
- Einführung klarer Mechanismen der Rechenschaftspflicht und Festlegung der für die KI-Governance zuständigen Personen.
- Planen Sie regelmäßige Mitarbeiterschulungen zu AI-Praktiken, -Protokollen und -Risiken, die sich auf praktische Szenarien konzentrieren.
- Aktualisierung der Leitlinien bei Aufkommen neuer KI-Tools.
- Erstellen Sie einen soliden Notfall- und Abhilfeplan für Datenverletzungen.

Kundenkommunikation über die Nutzung von AI

Transparenz ist die Grundlage einer effektiven Kundenkommunikation rund um den Einsatz von KI bei Buchhaltungsdienstleistungen. Die Unternehmen sollten proaktiv offenlegen, welche Buchhaltungsprozesse KI beinhalten, wie diese Technologien ihre Dienstleistungen erweitern und welche Sicherheitsvorkehrungen zum Schutz der Daten ihrer Kunden getroffen wurden.

Diese Angaben sollten in die Auftragsschreiben und Dienstleistungsvereinbarungen aufgenommen werden, um klare Erwartungen zu formulieren und Vertrauen beim Kunden zu schaffen.

Um den Bedenken der Kunden in Bezug auf KI zu begegnen, ist ein Ansatz erforderlich, der die berechtigten Fragen anerkennt und gleichzeitig durch konkrete Sicherheitsmaßnahmen für Sicherheit sorgt.

Die Unternehmen sollten darauf vorbereitet sein, ihre mehrschichtige Sicherheitsstrategie (Verschlüsselungsprotokolle, Zugangskontrollen usw.) zu erläutern und die menschliche Aufsicht zu betonen. Die Erstellung von Bildungsressourcen, wie FAQ oder Webinare, kann viel dazu beitragen, diese Technologien zu entmystifizieren und Missverständnisse auszuräumen.

Künftige Trends in der KI für das Rechnungswesen

Die Integration von generativer KI in Buchhaltungsworkflows ist einer der wichtigsten neuen Trends im Ökosystem der Buchhaltung und hat das Potenzial, die Art und Weise, wie Finanzfachleute mit Daten interagieren und Erkenntnisse gewinnen, radikal zu verändern. Im Gegensatz zu herkömmlichen Automatisierungswerkzeugen kann KI Erklärungen zu finanziellen Anomalien in natürlicher Sprache erstellen, vorläufige Prüfungsergebnisse entwerfen und kundenfertige Finanzberichte erstellen. Diese Fähigkeiten werden die Arbeit von Wirtschaftsprüfern wahrscheinlich in Richtung Überprüfung, Verfeinerung und strategische Interpretation verlagern, anstatt die Dokumentation von Grund auf zu erstellen. Wie bereits erwähnt, bringt die generative KI jedoch auch viele neue Sicherheitsherausforderungen mit sich.

Immer ausgefeiltere KI-Modelle werden die Fähigkeit von Wirtschaftsprüfungsunternehmen, Finanztrends zu prognostizieren, potenzielle Compliance-Probleme präventiv zu erkennen und Betrugsmuster mit größerer Genauigkeit aufzudecken, erheblich verbessern. All diese Fortschritte gehen mit wichtigen Sicherheitsaspekten einher Implikationen.

Da die Modelle bei der Erkennung von Mustern immer leistungsfähiger werden, werden sie auch zu wertvolleren Zielen für Cyberangreifer, die versuchen, Wettbewerbsinformationen zu gewinnen oder Finanzprognosen zu manipulieren. Dies erfordert noch sichereren Rahmen für KI-Systeme, die Daten verarbeiten.

KI im Bereich der Regulierungstechnologie (RegTech), die automatisch die Einhaltung der sich weiterentwickelnden Finanzvorschriften überwacht, stellt eine vielversprechende Perspektive für Buchhaltungsexperten dar. Diese Systeme können fortlaufend Aktualisierungen von Vorschriften in verschiedenen Rechtsordnungen überprüfen und Firmen auf relevante Änderungen aufmerksam machen, die ihre Kunden betreffen.

Da KI-Systeme immer autonomer werden, stellen sich Fragen zur Rechenschaftspflicht und zum angemessenen Gleichgewicht zwischen menschlichem und maschinellem Urteilsvermögen in Compliance-Angelegenheiten. KMPs müssen neue Fachkenntnisse in der KI-Prüfung und -Governance entwickeln, um diese neuen Gewässer effektiv zu navigieren.

EFAA
EUROPEAN FEDERATION OF ACCOUNTANTS AND AUDITORS FOR SMES

Über EFAA

Die Europäische Föderation der Buchhalter und Wirtschaftsprüfer für KMU ist ein Dachverband nationaler Buchhalter- und Wirtschaftsprüferorganisationen, deren einzelne Mitglieder professionelle Dienstleistungen hauptsächlich für KMU in der Europäischen Union und in Europa insgesamt erbringen. Sie wurde 1994 gegründet.

Die EFAA für KMU hat 15 Mitglieder in ganz Europa, die über 400.000 Buchhalter, Wirtschaftsprüfer und Steuerberater vertreten.

EFAA for SMEs ist Mitglied der Vereinigung von Handwerk und KMU (SME united) und Gründungsmitglied der European Financial Reporting Advisory Group (EFRAG).