

AI EN COMPTABILITÉ

Fédération européenne des comptables et auditeurs de PME

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



L'IA en comptabilité : Une introduction

L'IA est en train de révolutionner complètement la profession comptable. Les applications actuelles peuvent automatiser les tâches comptables de routine, telles que la tenue des comptes, les tests d'audit et l'analyse des données, ce qui permettrait aux PMO de gagner du temps pour apporter de la valeur ajoutée et fournir des services supplémentaires à leurs clients et se concentrer sur les activités stratégiques. Ces automatisations peuvent également réduire les erreurs humaines.

Malgré ses nombreux avantages, l'intégration de l'IA dans la comptabilité présente également des risques potentiels. Au premier rang de ceux-ci figurent les problèmes de sécurité des données et de protection de la vie privée.

Le secteur de la comptabilité se trouve à un moment critique où les entreprises doivent trouver un équilibre entre l'innovation et la prudence. Les outils avancés sont de plus en plus intégrés dans les systèmes comptables. Toutefois, les professionnels de la comptabilité doivent rester vigilants quant au maintien de l'intégrité des données, à la conformité réglementaire et à la préservation du contrôle humain.

Il s'agit du premier guide de l'EFAA sur l'utilisation de l'IA dans la comptabilité, qui met l'accent sur les aspects liés à la sécurité et à la protection de la vie privée. D'autres éditions sur d'autres sujets liés à l'IA sont prévues à l'avenir.

Confidentialité des données dans les systèmes comptables pilotés par l'IA

Lors de l'utilisation de l'IA en comptabilité, les données sensibles ne sont pas seulement des informations financières telles que les bilans et les flux de trésorerie, mais aussi des informations personnelles identifiables (PII) des clients, des employés et des fournisseurs. Les solutions d'IA traitent ces informations au moyen d'algorithmes élaborés qui analysent des modèles, prédisent des résultats et automatisent des tâches comptables de routine, d'où la nécessité d'intégrer des mesures de sécurité robustes.

Les mécanismes de stockage et de traitement des outils d'IA varient considérablement. Nombre d'entre eux fonctionnent sur des infrastructures basées sur l'informatique en nuage, où les données peuvent circuler entre plusieurs serveurs et juridictions. Les outils gratuits et largement utilisés peuvent très bien utiliser les données des clients pour l'entraînement des modèles, ce qui peut exposer des informations sensibles. Pour les comptes, il est essentiel de comprendre que la sécurité des données ne consiste pas seulement à prévenir les violations directes, mais aussi à contrôler la manière dont les informations circulent dans l'écosystème de l'IA, y compris les API, le stockage temporaire et les accords de traitement par des tiers.



EU Artificial Intelligence Act

Qu'est-ce que la loi sur l'IA ?

Outre le GDPR, l'UE a mis en place une autre législation essentielle qui a un impact significatif sur les organisations qui utilisent l'IA à des fins comptables.

La loi sur l'IA réglemente les technologies d'IA en fonction des niveaux de risque. Pour les cabinets comptables, cela signifie que les outils d'IA utilisés pour l'analyse financière, la détection des fraudes ou l'évaluation du crédit peuvent faire l'objet d'un examen plus approfondi et d'exigences de conformité.

"Il n'y a pas de temps à perdre pour adopter des règles visant à contrôler l'utilisation de l'IA."

- Margrethe Vestager, vice-présidente exécutive de la Commission européenne



Sélection de fournisseurs d'IA sécurisés pour la comptabilité

Lors du choix d'outils d'IA pour la comptabilité, les caractéristiques de sécurité doivent être une considération primordiale. Les PMC devraient privilégier les outils qui offrent des mesures de sécurité adéquates, notamment le chiffrement de bout en bout, des API sécurisées pour le transfert des données et des contrôles d'accès complets. Les solutions d'entreprise ont tendance à offrir des fonctions de sécurité meilleures et plus rigoureuses que les solutions gratuites destinées au grand public. Les outils d'IA "gratuits" doivent être abordés avec prudence, car ils fonctionnent souvent selon des modèles commerciaux où les données de l'utilisateur deviennent le produit.

Ils peuvent également conserver les données qui y sont saisies à des fins de formation des modèles. Les PSM devraient procéder à des évaluations approfondies des fournisseurs, notamment en examinant les certifications de sécurité (telles que SOC 2), en comprenant les politiques de résidence des données et en examinant les antécédents du fournisseur en matière de conformité. Les PMO devraient envisager des capacités d'IA intégrées dans des plateformes logicielles établies (telles que Co-Pilot dans Sage), car elles fonctionnent généralement dans des cadres de sécurité conçus pour les données financières.

Meilleures pratiques pour la protection des données des clients

L'anonymisation des données et les techniques de masquage constituent l'une des stratégies essentielles que les PSM peuvent employer. En supprimant (ou en cryptant) les informations personnellement identifiables avant qu'elles n'entrent dans les systèmes d'IA, on peut réduire considérablement le risque d'exposition des données sensibles des clients.

Ce processus peut être partiellement automatisé grâce à des outils d'IA qui identifient et expurgent les informations sensibles des documents financiers avant leur analyse. Il est évident que différents niveaux d'anonymisation des données peuvent être appropriés pour différents objectifs - de l'anonymisation complète pour l'analyse de modèles généraux à la pseudonymisation pour les flux de travail où une certaine capacité de réidentification doit être maintenue. Il existe également des techniques avancées (telles que la confidentialité différentielle) qui pourraient être mises en œuvre pour ajouter du "bruit" statistique aux ensembles de données tout en préservant leur valeur analytique.

Le cryptage est un élément de défense fondamental lorsqu'il s'agit de données comptables dans des systèmes d'IA. Les entreprises doivent mettre en œuvre un cryptage de qualité bancaire (AES-256 ou supérieur) pour toutes les données des clients et veiller à ce que les clés de cryptage soient gérées en toute sécurité. Lorsque des données sont transférées entre un logiciel de comptabilité et des outils d'analyse d'IA, des connexions API sécurisées (avec TLS 1.3 ou des protocoles équivalents) devraient être obligatoires. En règle générale, la mise en œuvre de contrôles d'accès stricts basés sur les rôles garantit que seul le personnel autorisé peut accéder à des types spécifiques de données clients.

Une stratégie proactive de protection des données des clients doit comprendre des évaluations régulières de la sécurité et une surveillance continue. La surveillance de la sécurité pilotée par l'IA peut détecter des schémas d'accès aux données inhabituels ou des violations potentielles en temps réel. En outre, les entreprises doivent conserver des pistes d'audit complètes de toutes les interactions de l'IA avec les données des clients.

Mise en œuvre d'une utilisation sûre de l'IA au sein de votre organisation

Comment élaborer une politique globale en matière d'intelligence artificielle ?

- Délimiter clairement les outils d'IA dont l'utilisation est approuvée.
- Spécifier les types de données qui peuvent y être saisies.
- Distinguer le traitement des informations confidentielles de celui des informations non confidentielles.
- Établir des mécanismes de responsabilité clairs, déterminer qui est responsable de la gouvernance de l'IA.
- Prévoir des sessions régulières de formation du personnel sur les pratiques, les protocoles et les risques liés à l'IA, en mettant l'accent sur des scénarios pratiques.
- Mettre à jour les lignes directrices au fur et à mesure de l'apparition de nouveaux outils d'IA.
- Mettre en place un solide plan d'urgence et de remédiation en cas de violation de données.



Communication avec les clients sur l'utilisation de l'IA

La transparence est le fondement d'une communication efficace avec les clients sur l'utilisation de l'IA dans les services comptables. Les cabinets devraient divulguer de manière proactive les processus comptables faisant appel à l'IA, la manière dont ces technologies améliorent leurs services et les garanties mises en place pour protéger les informations de leurs clients.

Ces informations devraient être intégrées au niveau des lettres de mission et des accords de service, ce qui permettrait de définir des attentes claires et d'établir la confiance avec le client.

Pour répondre aux préoccupations des clients concernant l'IA, il faut adopter une approche qui tienne compte des questions légitimes tout en rassurant par des mesures de sécurité concrètes.

Les entreprises doivent être prêtes à expliquer leur stratégie de sécurité à plusieurs niveaux (protocoles de cryptage, contrôles d'accès, etc.) et à mettre l'accent sur la surveillance humaine en place. La création de ressources éducatives, telles que des FAQ ou des webinaires, peut contribuer grandement à démystifier ces technologies et à dissiper les idées fausses.

Tendances futures de l'IA pour la comptabilité

L'intégration de l'IA générative dans les flux de travail comptables représente l'une des tendances émergentes les plus importantes dans l'écosystème comptable, avec le potentiel de transformer radicalement la façon dont les professionnels de la finance interagissent avec les données et génèrent des idées. Contrairement aux outils d'automatisation traditionnels, l'IA peut produire des explications en langage naturel sur les anomalies financières, rédiger des conclusions d'audit préliminaires et créer des rapports financiers prêts pour le client. Ces capacités vont probablement orienter le travail des comptables vers l'examen, l'affinage et l'interprétation stratégique plutôt que vers la rédaction de documents à partir de zéro. Toutefois, comme nous l'avons vu plus haut, l'IA générative pose également de nombreux nouveaux défis en matière de sécurité.

Des modèles d'IA de plus en plus sophistiqués amélioreront considérablement la capacité des cabinets comptables à prévoir les tendances financières, à identifier de manière préventive les problèmes de conformité potentiels et à détecter les schémas de fraude avec une plus grande précision. Toutes ces avancées s'accompagnent d'importantes mesures de sécurité implications.

À mesure que les modèles deviennent plus puissants pour identifier des schémas, ils deviennent également des cibles plus précieuses pour les cyberattaquants qui cherchent à extraire des informations sur la concurrence ou à manipuler des prédictions financières. Cela nécessitera des cadres encore plus sécurisés autour des systèmes d'IA qui traitent les données.

L'IA de la technologie réglementaire (RegTech) qui surveille automatiquement la conformité avec les réglementations financières en évolution représente des perspectives prometteuses pour les professionnels de la comptabilité. Ces systèmes peuvent analyser en permanence les mises à jour réglementaires dans plusieurs juridictions et alerter les entreprises sur les changements pertinents qui affectent leurs clients.

Alors que les systèmes d'IA deviennent de plus en plus autonomes, des questions se posent sur la responsabilité et l'équilibre approprié entre le jugement humain et celui de la machine en matière de conformité. Les PSM devront développer une nouvelle expertise en matière d'audit et de gouvernance de l'IA pour naviguer efficacement dans ces nouvelles eaux.



À propos de l'EFAA

La Fédération européenne des experts-comptables et des réviseurs d'entreprises pour les PME est une organisation qui regroupe les organisations nationales d'experts-comptables et de réviseurs d'entreprises dont les membres individuels fournissent des services professionnels principalement aux PME au sein de l'Union européenne et de l'Europe dans son ensemble. Elle a été fondée en 1994.

L'EFAA pour les PME compte 15 membres dans toute l'Europe, représentant plus de 400 000 comptables, auditeurs et conseillers fiscaux.

L'EFAA for SMEs est membre de l'association de l'artisanat et des PME (SME united) et membre fondateur du Groupe consultatif pour l'information financière en Europe (EFRAG).