

AI IN ACCOUNTING

Europese Federatie van Accountants en Bedrijfsrevisoren voor het MKB

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



AI in ACCOUNTING: Een inleiding

AI zorgt voor een complete revolutie in het accountantsberoep. De huidige toepassingen kunnen routinematige boekhoudtaken automatiseren, zoals boekhouden, controle testen en gegevensanalyse, waardoor SMP's tijd kunnen besparen om waarde toe te voegen en extra diensten te leveren aan hun klanten en zich kunnen richten op strategische activiteiten. Deze automatiseringen kunnen ook menselijke fouten verminderen.

Ondanks de vele voordelen brengt de integratie van AI in de boekhouding ook potentiële risico's met zich mee. Een van deze risico's is de beveiliging van gegevens en privacy.

De boekhoudsector bevindt zich op een kritiek punt waar bedrijven een evenwicht moeten vinden tussen innovatie en voorzichtigheid. Er worden steeds meer geavanceerde tools geïntegreerd in boekhoudsystemen. Accountants moeten echter waakzaam blijven om de integriteit van gegevens te behouden, naleving van regelgeving te garanderen en menselijk toezicht te behouden.

Dit is EFAA's eerste gids over het gebruik van AI in de accountancy, met de nadruk op beveiligings-/privacyaspecten. Verdere uitgaven over andere AI-onderwerpen zijn voorzien in de toekomst.

Gegevensprivacy in AI-gestuurde boekhoudsystemen

Bij het gebruik van AI in de boekhouding zijn gevoelige gegevens niet alleen financiële informatie zoals balansen en kasstroomoverzichten, maar ook persoonlijk identificeerbare informatie (PII) van klanten, werknemers en leveranciers. AI-oplossingen verwerken deze informatie via uitgebreide algoritmen die patronen analyseren, uitkomsten voorspellen en routinematige boekhoudtaken automatiseren, waardoor het essentieel is om robuuste beveiligingsmaatregelen te nemen.

De opslag- en verwerkingsmechanismen van AI-tools variëren aanzienlijk. Veel tools werken op cloudgebaseerde infrastructuren, waarbij gegevens over meerdere servers en jurisdicties kunnen reizen. Gratis en veelgebruikte tools kunnen klantgegevens gebruiken voor modeltraining, waardoor mogelijk gevoelige informatie wordt blootgelegd. Voor accounts is het cruciaal om te begrijpen dat gegevensbeveiliging niet alleen gaat over het voorkomen van directe inbreuken, maar ook over het beheersen van de manier waarop informatie door het AI-ecosysteem stroomt, inclusief API's, tijdelijke opslag en verwerkingsovereenkomsten met derden.



EU Artificial Intelligence Act

Wat is de AI-wet?

Naast de GDPR heeft de EU nog een andere cruciale wetgeving opgesteld die van grote invloed is op organisaties die AI gebruiken voor boekhoudkundige doeleinden.

De AI-wet reguleert AI-technologieën op basis van risiconiveaus. Voor accountantskantoren betekent dit dat AI-tools die worden gebruikt voor financiële analyse, fraudedetectie of kredietbeoordeling aan strenger toezicht en strengere compliance-eisen kunnen worden onderworpen.

"Er is geen tijd te verliezen met het aannemen van regels om het gebruik van AI te controleren."

- Margrethe Vestager, uitvoerend vicevoorzitter van de Europese Commissie



Veilige AI-aanbieders selecteren voor boekhouding

Bij het kiezen van AI-tools voor boekhoudkundig gebruik moeten beveiligingsfuncties een primaire overweging zijn. SMP's moeten de voorkeur geven aan tools die adequate beveiligingsmaatregelen bieden, waaronder end-to-end encryptie, veilige API's voor gegevensoverdracht en uitgebreide toegangscontroles. Bedrijfsoplossingen bieden vaak betere en strengere beveiligingsfuncties dan gratis consumentgerichte alternatieven. De 'gratis' AI tools moeten met voorzichtigheid worden benaderd, omdat deze vaak werken op basis van bedrijfsmodellen waarbij gebruikersgegevens het product worden.

Ze kunnen de ingevoerde gegevens ook bewaren voor modeltrainingsdoeleinden. SMP's moeten een grondige beoordeling van de leverancier uitvoeren, inclusief het bekijken van beveiligingscertificeringen (zoals SOC 2), het begrijpen van het beleid voor het verblijf van gegevens en het onderzoeken van de nalevingsgeschiedenis van de leverancier. SMP's moeten AI-mogelijkheden overwegen die geïntegreerd zijn in gevestigde softwareplatforms (zoals Co-Pilot in Sage), omdat deze doorgaans werken binnen beveiligingskaders die ontworpen zijn voor financiële gegevens.

Beste praktijken voor het beschermen van klantgegevens

Een van de essentiële strategieën die SMP's kunnen toepassen, zijn technieken voor het anonimiseren en maskeren van gegevens. Door persoonlijk identificeerbare informatie te verwijderen (of te versleutelen) voordat deze in AI-systemen terechtkomt, kan het risico op blootstelling van gevoelige klantgegevens drastisch worden verminderd.

Dit proces kan gedeeltelijk worden geautomatiseerd met behulp van AI-tools die gevoelige informatie uit financiële documenten identificeren en redigeren vóór analyse. Het is duidelijk dat verschillende niveaus van anonimisering van gegevens geschikt kunnen zijn voor verschillende doeleinden - van volledige anonimisering voor algemene patroonanalyse tot pseudonimisering voor workflows waarbij enige mogelijkheid tot heridentificatie moet worden behouden. Er zijn ook geavanceerde technieken (zoals differentiële privacy) die kunnen worden geïmplementeerd om statistische 'ruis' toe te voegen aan datasets met behoud van hun analytische waarde.

Encryptie is een fundamenteel verdedigingsonderdeel als het gaat om boekhoudgegevens in AI-systemen. Bedrijven moeten encryptie van bankkwaliteit (AES-256 of hoger) implementeren voor alle klantgegevens en ervoor zorgen dat encryptiesleutels veilig worden beheerd. Wanneer gegevens worden verplaatst tussen boekhoudsoftware en AI-analysetools, moeten veilige API-verbindingen (met TLS 1.3 of gelijkwaardige protocollen) verplicht zijn. Als algemene regel geldt dat het implementeren van strikte rolgebaseerde toegangscontroles ervoor zorgt dat alleen geautoriseerd personeel toegang heeft tot specifieke soorten cliëntgegevens.

Een proactieve strategie voor de bescherming van klantgegevens moet regelmatige beveiligingsbeoordelingen en voortdurende bewaking omvatten. AI-gestuurde beveiligingsmonitoring kan ongebruikelijke gegevenstoegangspatronen of potentiële inbreuken in realtime detecteren. Daarnaast moeten bedrijven volledige controletrajecten bijhouden van alle AI-interacties met klantgegevens.

Veilig AI-gebruik implementeren binnen uw organisatie

Hoe ontwikkel je een uitgebreid AI-beleid?

- Duidelijk afbakenen welke AI-tools goedgekeurd zijn voor gebruik.
- Specificeer de soorten gegevens die erin kunnen worden ingevoerd.
- Onderscheid maken tussen de behandeling van vertrouwelijke en niet-vertrouwelijke informatie.
- Duidelijke verantwoordingsmechanismen vaststellen en bepalen wie verantwoordelijk is voor AI-governance.
- Plan regelmatig trainingen voor medewerkers over AI-praktijken, protocollen en risico's, waarbij de nadruk ligt op praktische scenario's.
- Werk richtlijnen bij als er nieuwe AI-tools verschijnen.
- Een robuust nood- en herstelplan voor datalekken opstellen.



Communicatie met klanten over AI-gebruik

Transparantie is de basis van effectieve communicatie met klanten over het gebruik van AI in accountancydiensten. Bedrijven moeten proactief bekendmaken bij welke boekhoudprocessen AI wordt gebruikt, hoe deze technologieën hun dienstverlening verbeteren en welke waarborgen er zijn om de informatie van hun klanten te beschermen.

Deze toelichtingen moeten worden opgenomen op het niveau van de opdrachtbevestiging en dienstverleningsovereenkomsten, zodat duidelijke verwachtingen worden gecreëerd en vertrouwen wordt opgebouwd bij de klant.

Om de bezorgdheid van klanten over AI weg te nemen, is een aanpak nodig waarbij legitieme vragen worden erkend en tegelijkertijd zekerheid wordt geboden door middel van concrete beveiligingsmaatregelen.

Bedrijven moeten bereid zijn om hun meerlagige beveiligingsstrategie uit te leggen (encryptieprotocollen, toegangscontroles, etc.) en om het menselijke toezicht te benadrukken. Het creëren van educatieve middelen, zoals FAQ's of webinars, kan een grote bijdrage leveren aan het demystificeren van deze technologieën en het wegnemen van misvattingen.

Toekomstige trends in AI voor de boekhouding

De integratie van generatieve AI in boekhoudkundige workflows is een van de belangrijkste opkomende trends in het boekhoudkundige ecosysteem, met het potentieel om de manier waarop financiële professionals met gegevens omgaan en inzichten genereren radicaal te veranderen. In tegenstelling tot traditionele automatiseringstools kan AI verklaringen in natuurlijke taal produceren voor financiële afwijkingen, voorlopige auditbevindingen opstellen en financiële rapporten maken die klaar zijn voor de klant. Door deze mogelijkheden zal het werk van accountants waarschijnlijk meer gericht zijn op beoordeling, verfijning en strategische interpretatie dan op het opstellen van documentatie vanaf nul. Zoals hierboven besproken, brengt generatieve AI echter ook veel nieuwe beveiligingsuitdagingen met zich mee.

Dankzij steeds geavanceerdere AI-modellen zullen accountantskantoren aanzienlijk beter in staat zijn om financiële trends te voorspellen, preventief potentiële nalevingsproblemen te identificeren en fraudepatronen nauwkeuriger te detecteren. Al deze vooruitgang gaat gepaard met belangrijke veiligheidsmaatregelen gevolgen.

Naarmate modellen krachtiger worden in het identificeren van patronen, worden ze ook waardevollere doelwitten voor cyberaanvallers die informatie over concurrenten willen ontfutselen of financiële voorspellingen willen manipuleren. Dit vereist nog veiligere kaders rond AI-systemen die gegevens verwerken.

Regelgevingstechnologie (RegTech) AI die automatisch toeziet op de naleving van veranderende financiële regelgeving biedt veelbelovende vooruitzichten voor boekhoudprofessionals. Deze systemen kunnen voortdurend regelgevingsupdates in verschillende rechtsgebieden scannen en bedrijven waarschuwen voor relevante wijzigingen die van invloed zijn op hun klanten.

Nu AI-systemen steeds autonoom worden, rijzen er vragen over verantwoordingsplicht en de juiste balans tussen menselijke en machinale oordeelsvorming in compliancekwesties. SMP's zullen nieuwe expertise in AI-auditing en -governance moeten ontwikkelen om deze nieuwe wateren effectief te kunnen bevaren.



Over EFAA

De European Federation of Accountants and Auditors for SMEs is een overkoepelende organisatie voor nationale accountants- en auditorsorganisaties waarvan de individuele leden voornamelijk professionele diensten verlenen aan KMO's binnen de Europese Unie en Europa als geheel. Ze werd opgericht in 1994.

EFAA for SMEs heeft 15 leden in heel Europa die meer dan 400.000 accountants, auditors en belastingadviseurs vertegenwoordigen.

EFAA for SMEs is lid van de vereniging van ambachten en het MKB (SME united) en een stichtend lid van de European Financial Reporting Advisory Group (EFRAG).