A Short Guide to Privacy, Security, and Best Practices

AI IN ACCOUNTING

European Federation of Accountants and Auditors for SMEs   +32 (0)2 736 88 86 | secretariat@efaa.com | www.efaa.com

AI in Accounting: An Introduction

AI is completely revolutionizing the accounting profession. Current applications can automate routine accounting tasks, such as bookkeeping, audit testing and data analysis, which would save SMPs time to add value and provide additional services to their clients and focus on strategic activities. These automations can also reduce human error.

Despite its many benefits, the integration of AI in accounting also introduces potential risks. Primary among these are data security and privacy concerns.

The accounting industry is at a critical juncture where firms must balance innovation with caution. Advanced tools are increasingly being integrated into accounting systems. However, accounting professionals must remain vigilant about maintaining data integrity, ensuring regulatory compliance and preserving human oversight.

This is EFAA's initial guide around AI usage in accounting, focusing on security/privacy aspects. Further editions around other AI topics are foreseen in the future.

Data Privacy in AI-Driven Accounting Systems

When using AI in accounting, sensitive data isn't just financial information such as balance sheets and cash flow records, but also personally identifiable information (PII) of clients, employees, and vendors. AI solutions process this information through elaborate algorithms that analyze patterns, predict outcomes, and automate routine accounting tasks, making it essential to incorporate robust security measures.

Storage and processing mechanisms among AI tools vary significantly. Many operate on cloud-based infrastructures, where data may travel across multiple servers and jurisdictions. Free and widely used tools may well use client data for model training, potentially exposing sensitive information. For accounts, it's crucial to understand that data security isn't just about preventing direct breaches, but also about controlling how information flows through the AI ecosystem, including APIs, temporary storage, and 3rd-party processing arrangements.

EU Artificial Intelligence Act

What is the AI Act?

Besides the GDPR, the EU has established another pivotal legislation that significantly impacts organizations that use AI for accounting purposes.

The AI Act regulates AI technologies based on risk levels. For accounting firms, this means that AI tools used for financial analysis, fraud detection, or credit assessment may be subject to enhanced scrutiny and compliance requirements.

> **"There is no time to waste on passing rules to control the use of AI."**
>
> — **Margrethe Vestager**, Executive Vice-President of the European Commission

Selecting Secure AI Providers for Accounting

When choosing AI tools for accounting use, security features should be a primary consideration. SMPs should prioritize tools that offer adequate security measures including end-to-end encryption, secure APIs for data transfer, and comprehensive access controls. Enterprise solutions tend to provide better and more rigorous security features than free consumer-oriented alternatives. The 'free' AI tools should be approached with caution, as these often operate on business models where user data becomes the product.

They may also retain the data entered into them for model training purposes. SMPs should conduct thorough vendor assessments that include reviewing security certifications (such as SOC 2), understanding data residency policies, and examining the provider's compliance history.

SMPs should consider AI capabilities that are integrated into established software platforms (such as Co-Pilot in Sage), as these typically operate within security frameworks designed for financial data.

Best Practices for Protecting Client Data

One of the essential strategies SMPs can employ include data anonymization and masking techniques. By removing (or encrypting) personally identifiable information before it enters AI systems, one can dramatically reduce the risk of exposing sensitive client data.

This process can be partially automated through AI tools that identify and redact sensitive information from financial documents before analysis. It's obvious that different levels of anonymization of data may be appropriate for different purposes – from complete anonymization for general pattern analysis to pseudonymization for workflows where some reidentification capability must be maintained. There are also advanced techniques (such as differential privacy) that could be implemented to add statistical 'noise' to datasets while preserving their analytical value.

Encryption is a fundamental defense component when it comes to accounting data in AI systems. Firms should implement bank-grade encryption (AES-256 or higher) for all client data and ensure that encryption keys are securely managed. When data is moved between accounting software and AI analysis tools, secure API connections (with TLS 1.3 or equivalent protocols) should be mandatory. As a general rule, implementing strict role-based access controls ensures that only authorized personnel can access specific types of client data.

A proactive client data protection strategy should include regular security assessments and continuous monitoring. AI-driven security monitoring can detect unusual data access patterns or potential breaches in real-time. Additionally, firms should maintain complete audit trails of all AI interactions with client data.

Implementing Safe AI Usage Within Your Organization

How to develop a comprehensive AI policy:

- Clearly delineate which AI tools are approved for use.
- Specify the types of data that can be entered in them.
- Distinguish between handling confidential and non-confidential information.
- Establish clear accountability mechanisms, identify who is responsible for AI governance.
- Plan regular staff training sessions on AI practices, protocols, and risks, focusing on practical scenarios.
- Update guidelines as new AI tools emerge.
- Set up a robust data breach contingency and remediation plan.

Client Communication About AI Usage

Transparency is the foundation of effective client communication around AI usage in accounting services. Firms should proactively disclose which accounting processes involve AI, how these technologies augment their service, and what safeguards are in place to protect their clients' information.

These disclosures should be incorporated at the level of engagement letters and service agreements, thus setting clear expectations and establishing trust with the client.

Addressing client concerns about AI requires an approach that acknowledges legitimate questions while providing reassurance through concrete security measures.

Firms should be prepared to explain their multi-layered security strategy (encryption protocols, access controls, etc.) as well as emphasize the human oversight in place. Creating educational resources, such as FAQ or webinars, can go a long way to help demystify these technologies and address misconceptions.

Future Trends in AI for Accounting

The integration of Generative AI into accounting workflows represents one of the most significant emerging trends in the accounting ecosystem, with the potential to radically transform how financial professionals interact with data and generate insights. Unlike traditional automation tools, AI can produce natural language explanations of financial anomalies, draft preliminary audit findings, and create client-ready financial reports. These capabilities will likely shift accountants' work towards review, refinements, and strategic interpretation rather than drafting documentation from scratch. However, as discussed above, generative AI also introduces many new security challenges.

Increasingly sophisticated AI models will siginificantly enhance accounting firms' ability to forecast financial trends, preemptively identify potential compliance issues, and detect fraud patterns with greater accuracy. All these advances come with important security implications.

As models become more powerful at identifying patterns, they also become more valuable targets for cyber attackers seeking to extract competitive intelligence or manipulate financial predictions. This will necessitate even more secure frameworks around AI systems that handle data.

Regulatory technology (RegTech) AI that automatically monitors compliance with evolving financial regulations represents promising prospects for accounting professionals. These systems can continuously scan regulatory updates across multiple jurisdictions and alert firms to relevant changes that affect their clients.

As AI systems are becoming more autonomous, questions arise about accountability and the appropriate balance between human and machine judgment in compliance matters. SMPs will need to develop new expertise in AI auditing and governance to navigate these new waters effectively.

EFAA
EUROPEAN FEDERATION OF ACCOUNTANTS AND AUDITORS FOR SMES

About EFAA

The European Federation of Accountants and Auditors for SMEs is an umbrella organization for national accountants and auditors' organizations whose individual members provide professional services primarily to SMEs within the European Union and Europe as a whole. It was founded in 1994.

EFAA for SMEs has 15 members throughout Europe representing over 400,000 accountants, auditors and tax advisors.

EFAA for SMEs is a member of the association of crafts and SMEs (SME united) and a founding member of the European Financial Reporting Advisory Group (EFRAG).