



## Security & Privacy Overview for Our Excel Add-In

### Introduction

We understand that the privacy and security of your data are of the utmost importance, especially when dealing with sensitive accounting workpapers. Our Excel add-in is designed with robust security practices to ensure that your information remains safe. This document explains how our add-in interacts with OpenAI through their API and outlines the privacy protections in place.

### How Our Add-In Works

Our Excel add-in integrates with OpenAI's API to assist in reviewing accounting workpapers. Here's how the process works:

1. **Data Submission:** When you use the add-in, specific pieces of data from your Excel workbook are sent to OpenAI's servers through a secure API connection.
2. **Processing:** The OpenAI API processes the submitted data and provides the relevant analysis or response.
3. **Results:** The processed response is returned to your Excel workbook for your use.

### Privacy Protections

We take data privacy very seriously. Here's what you need to know:

- **Data Handling by OpenAI:** OpenAI processes the data solely for providing you with the requested response. Your data is not used for any other purpose beyond fulfilling the API request. No data submitted through the API is used for training OpenAI models (see discussions at <https://openai.com/enterprise-privacy/>)
- **Data Retention by OpenAI:** OpenAI's API does not retain data from API interactions for longer than necessary.<sup>1</sup> Data is not stored permanently by OpenAI; it is used to generate a response and then discarded.
- **No Data Sent to Us:** The data you submit is never sent to us. We have no access to the data that is processed by OpenAI. All interactions occur strictly between your Excel workbook and OpenAI's API.

### Security Measures

- **Encryption:** Data is encrypted both in transit and at rest. When your data is sent from Excel to OpenAI and back, it is encrypted using industry-standard HTTPS protocols to prevent unauthorized access.

---

<sup>1</sup> "Except for certain endpoints and features listed in our [platform documentation](#), OpenAI may securely retain API inputs and outputs for up to 30 days to provide the services and to identify abuse. After 30 days, API inputs and outputs are removed from our systems, unless we are legally required to retain them. You can also request zero data retention (ZDR) for eligible endpoints if you have a qualifying use-case. For details on data handling, visit our [Platform Docs](#) page." (see <https://openai.com/enterprise-privacy/>).

- **Access Control:** Only authorized users can interact with the add-in and make API calls, ensuring your data remains secure.

### **OpenAI's Privacy & Security Practices**

For additional details about OpenAI's security and privacy practices, you can refer to their official policies:

- [OpenAI Privacy Policy](#)
- [OpenAI Security Overview](#)
- [OpenAI Security Portal](#) – lists the SOC 2, 3, GDPR, and additional compliance documentation.

These links provide a comprehensive overview of how OpenAI handles data, their approach to privacy, and the measures they take to maintain a secure environment.

### **Future Versions**

Currently, we are testing a beta version of the product that utilizes the OpenAI API to perform the workpaper review. The final version of the product is designed to be flexible and can be customized to work with other Generative AI APIs. For example, if you have an enterprise license for Microsoft Copilot that includes API access, we can configure the tool to use that API, ensuring it benefits from the security and compliance features of Microsoft's platform.

### **Our Commitment**

We are committed to ensuring that your data is handled with the utmost care and attention to privacy. If you have any questions or concerns regarding the security of your information, please do not hesitate to reach out to us.