



# Risk Assessment for Copilots in Power Platform

Carsten Groth

20 March 2024



# How to prepare for AI

"Security and risk management leaders must implement verifiable controls for AI data protection, privacy, application security and filtering of large language model content inputs and outputs."

- Gartner

Gartner, Quick Answer: How to Make Microsoft 365 Copilot Enterprise-Ready From a Security and Risk Perspective,, Avivah Litan, Matt Cain, Jeremy D'Hoinne, Nader Henein, Dennis Xu, 15 September 2023

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

eXalent

365<sup>°</sup>  
training

POWER  
PLATFORM 24

# A copilot for almost every Power Platform experience

And there's more to come...



## Copilot in Power Apps Studio

Copilot to assist building and editing your apps.



## Copilot in Power Pages Designer

Copilot to assist building and editing your web pages.



## Copilot for Power Apps apps

Copilot chat for canvas apps running in web browser. Copilot for model-driven apps.



## Copilot in Power Automate

Copilot to assist building and editing a cloud flow.



## Copilot for drafting text

Copilot to generate deployment notes and app descriptions.  
Copilot to assist with text input in canvas apps web player.

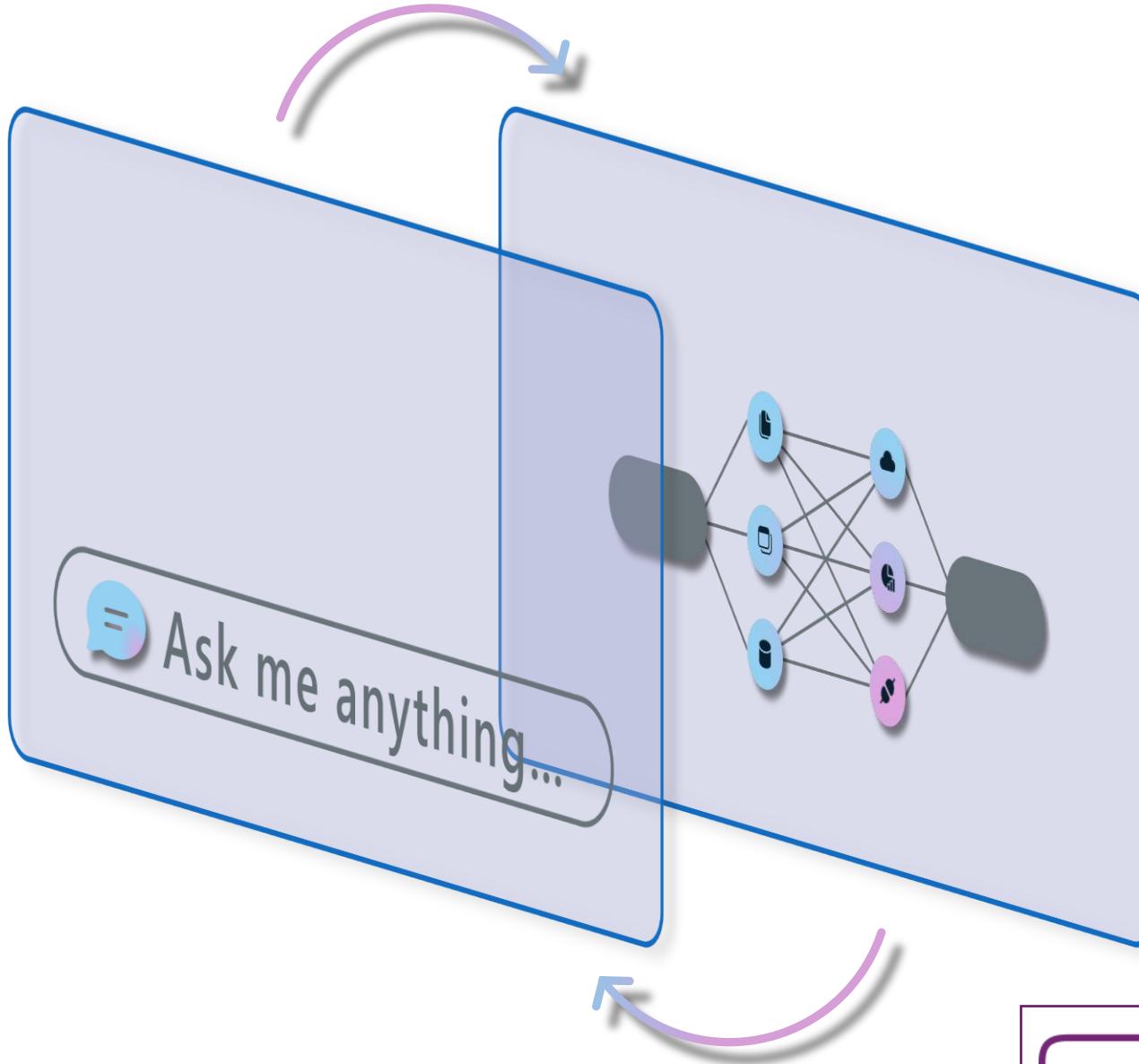


## Copilot in Power Automate for Desktop

Copilot to assist with product-related questions

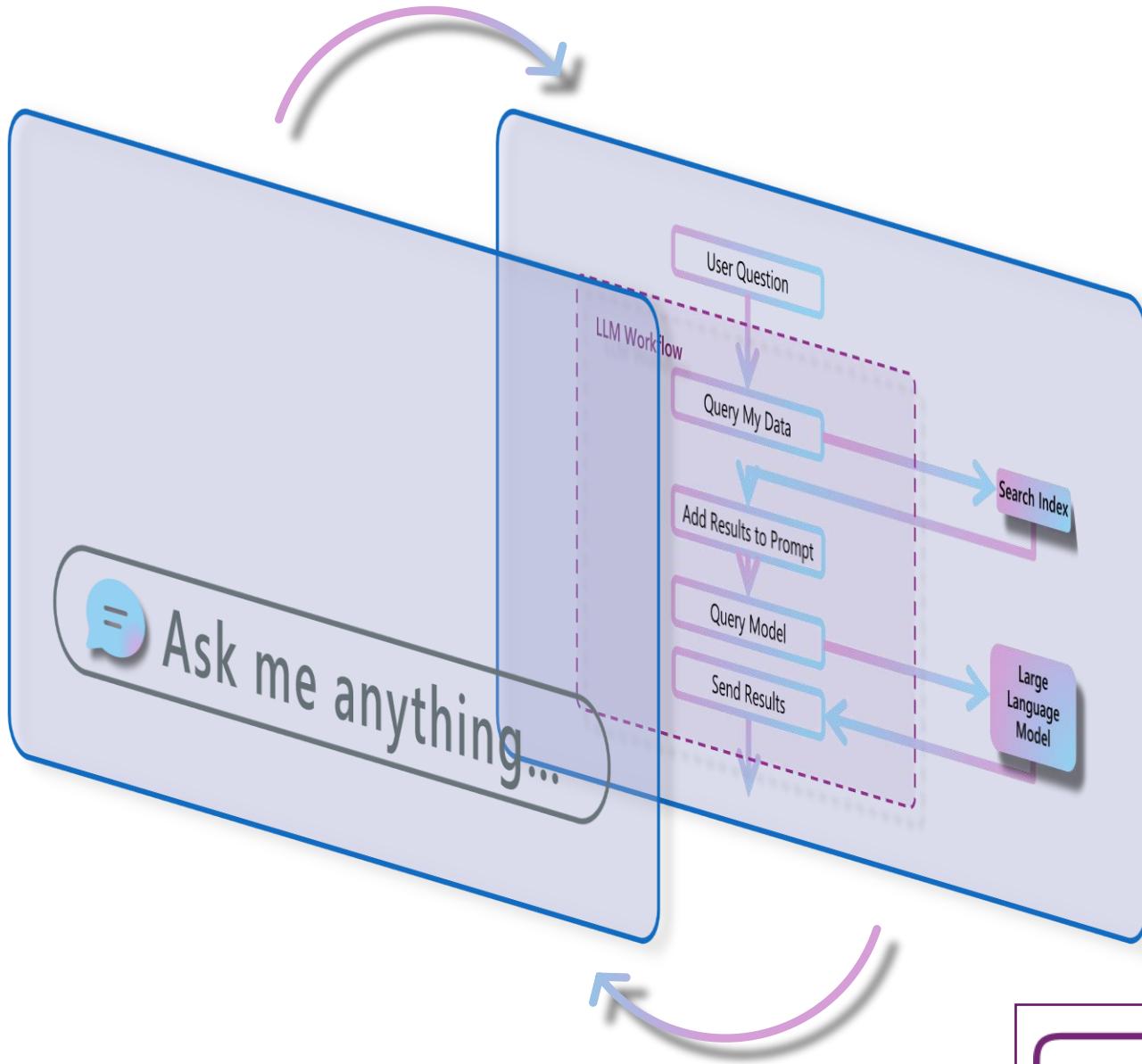


Natural  
user interface



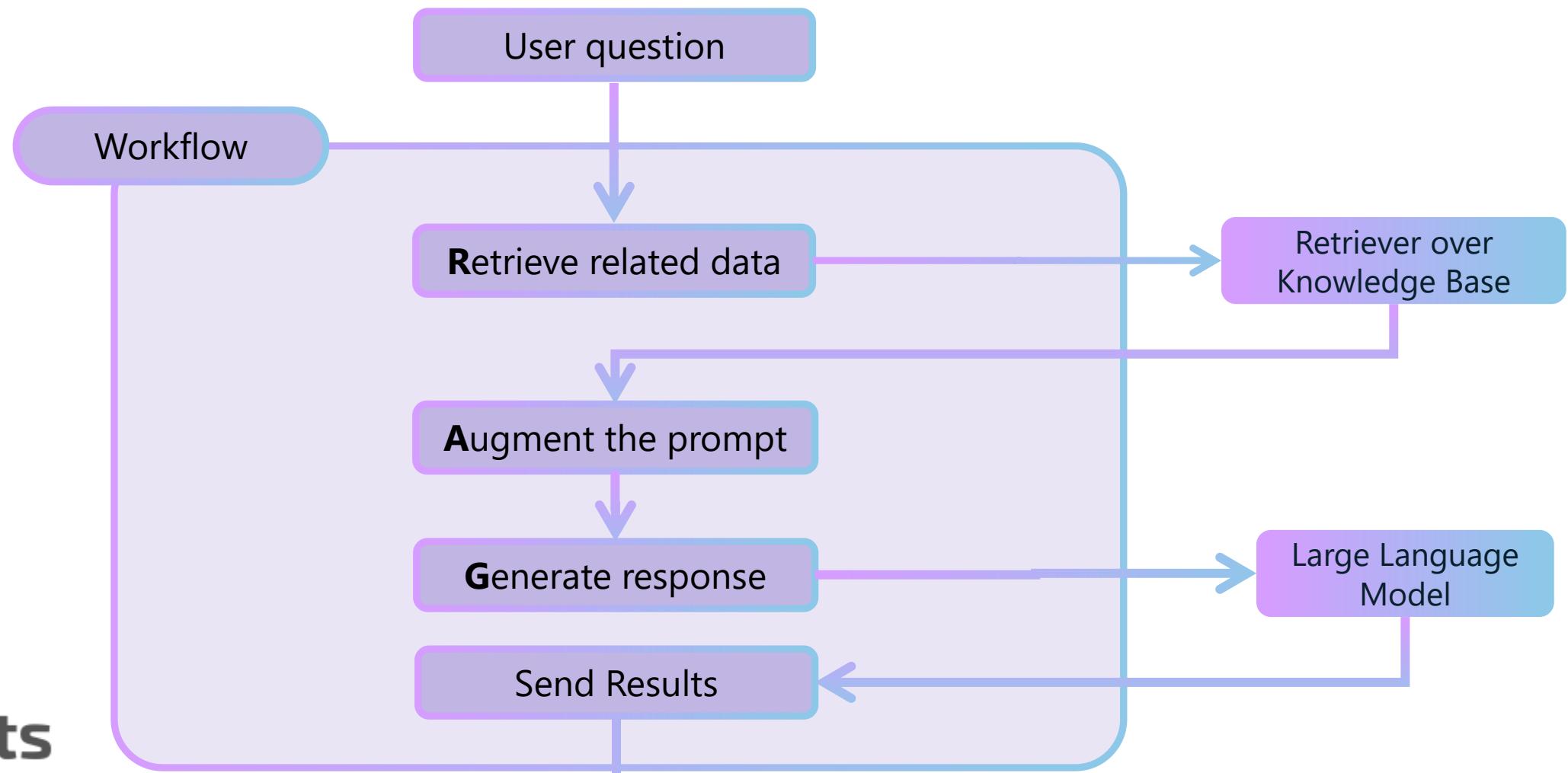
Reasoning  
engine

Natural user interface



Retrieval  
Augmented  
Generation

# Retrieval Augmented Generation (RAG)



# Let's build an app. What should it do?

Collect RSVPs

Track sales leads

List inventory

Manage inspections

Use everyday words to describe what your app should collect, track, list, or manage ...

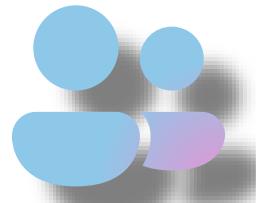


## Demo Time

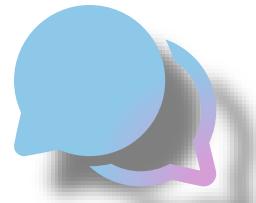


This feature uses generative AI. [See terms](#)

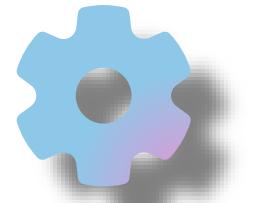
# AI transformation opportunities



Enrich  
employee  
experiences



Reinvent  
customer  
engagement



Reshape  
business  
processes



Bend the  
curve on  
innovation

# Innovate confidently with a responsible AI platform

Safeguard your organization, employees, and data with a cloud that runs on trust.

Build on security and privacy-compliant infrastructure that is purpose-built for AI at scale.

Grow with a partner committed to putting responsible AI into action with principles, practices, and tools.

eXalents

**365<sup>°</sup>**  
training



# Evaluation matrix

## Groundedness

Do the model's generated answers align with information from the input source

## Relevance

Is the model's generated response relevant for given question

## Coherence

Does the language model produce output that resembles human-like language

Microsoft  
protects your  
data and  
enables you to  
control it

## Protecting your data



### Security and Compliance



### Data Usage and Privacy



### Committed to responsible AI



## Inheriting Power Platform & M365 policies and controls



### Data access & permissions



### User-tenant focus



### Customer data protection



### Data processing and residency

# Power Platform Copilot Governance (Tenant level)

- 1 Control Copilot in Power Apps for building apps and answers to questions
- 2 Control Copilot in Power Automate via Azure OpenAI and Bing Search
- 3 Control 'generative answers' in Microsoft Copilot Studio
- 4 Participate in improving the LLMs. We don't use customer data to train Azure OpenAI Service foundation models.

1 Copilot in Power Apps Preview X

Allow people to use AI to help build apps and get answers to questions. Currently in preview. [Learn more](#)

On

2 Copilot help assistance in Power Automate via Bing Preview X

The Copilot generative answers capability is powered by Azure OpenAI and Bing Search and is currently available only in US-Based environments. [Learn more](#)

By using this feature you consent that your data will flow to Bing which operates outside the Power Automate compliance and geographical boundaries. ([Terms & conditions](#))

On

3 Publish bots with AI features X

Allow bot authors to publish Power Virtual Agents bots when AI features are enabled, like conversational boosting with generative answers. [Learn more](#)

You agree to the [supplemental terms](#) when this feature is enabled.

Enabled

4 Data sharing for Dynamics 365 Copilot and Power Platform Copilot AI Features X

Terms of Service

Allow Microsoft to capture and human review inputs and outputs from Copilot AI features to build, improve and/or validate Microsoft's machine learning models, features, service, and related systems. Requires agreement to the [supplemental terms](#). Data is not shared when Copilot AI features are turned off. [Learn more](#)

Enable Data Sharing

Enabled

# Power Platform Copilot Governance (Environment level)

- 1 Control Copilot for canvas editors and Copilot chat experience for end-user

**1 Copilot** A Preview

Allow canvas editors to get AI-powered answers to how-to questions and AI Builder GPT experiences. Currently in preview. [Learn more](#)

On

Allow users to analyze data using an AI-powered chat experience in [canvas](#) and [model-driven apps](#). [Learn more](#)

Default

- 2 Control AI Builder models and using AI in formula columns

**2 AI Builder**

Enable the usage of model types that are in preview [Learn more](#)

AI Builder preview models

On

**AI suggestions for formula columns** A Preview

Allow users to get AI suggestions when creating formula columns. Currently in preview. [Learn more](#)

Off

- 3 Opt-in on access of Copilot for each environment when outside US, UK, and Australia

**3 Generative AI features** X

Agree to the following terms to enable generative AI features. [Learn More](#)

**Move data across regions**

Terms of use for data movement across geographical data boundaries

I understand that generative AI features use the Azure OpenAI Service. By using them, I agree to my data being stored and processed by the Azure OpenAI Service outside of my environment's geographic region or compliance boundary. [See terms](#)

**Bing Search**

Terms of use for Bing Search

I understand that some generative AI features use Bing Search. Your data will flow outside your organization's compliance and geo boundaries. Customer's use of Bing Search is governed by the [Microsoft Services Agreement](#) and the [Microsoft Privacy Statement](#).

**PLATFOR** ZT

# Potential harms with generative AI

- Ungrounded outputs & errors
- Jailbreaks & prompt injection attacks
- Harmful content & code
- Manipulation and human-like behavior

eXalents

**365<sup>+</sup>**  
training



# Microsoft enterprise AI safeguard



Your data is your data



Your data is not used to train or enrich foundation AI models



Your data and AI models are protected at every step



Our Customer Copyright Commitment

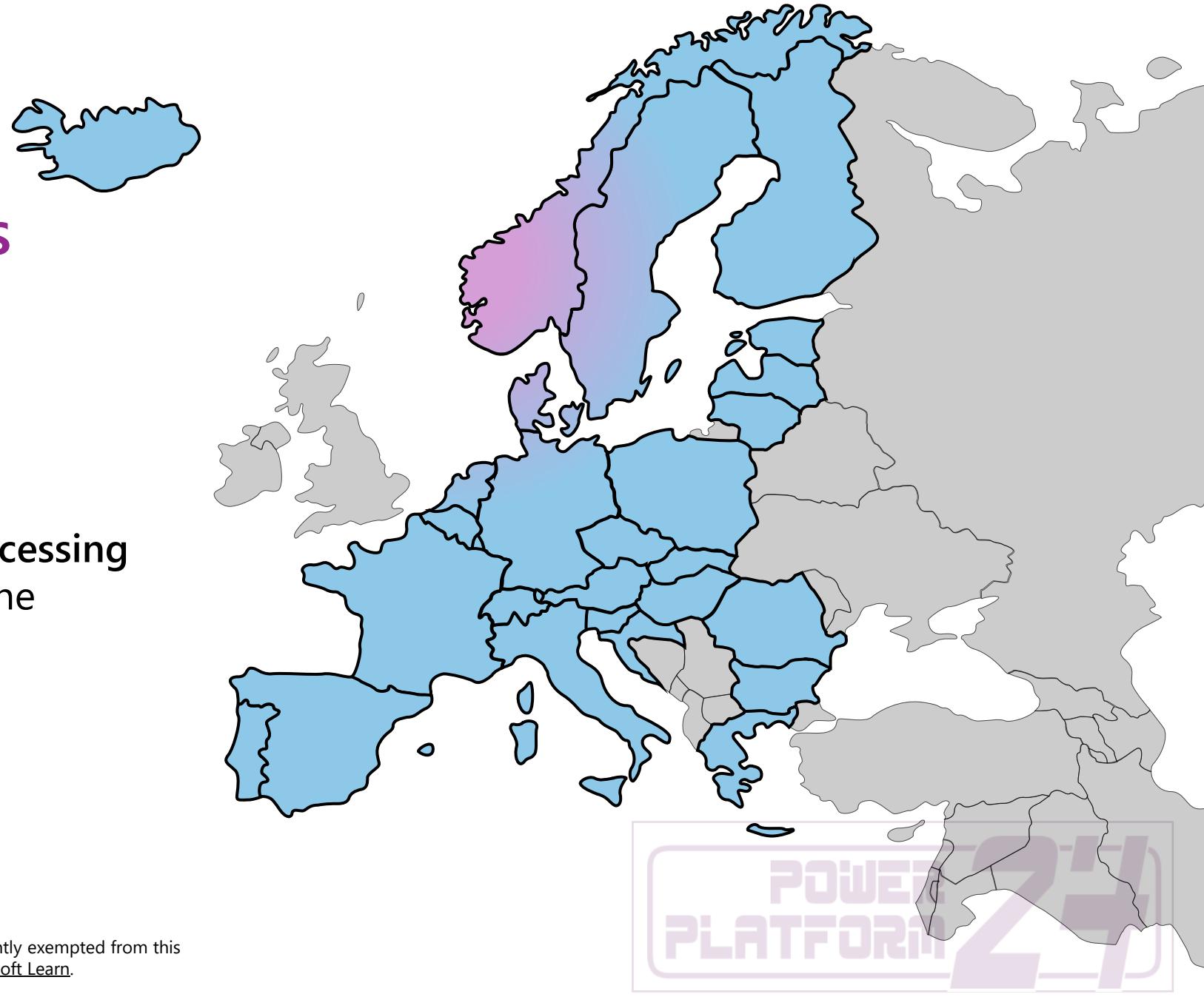
eXalents

**365<sup>°</sup>**  
training



# The EU Data Boundary provides more expansive commitments

EUDB terms provide contractual commitments for storing and processing EU + EFTA customer data within the European Union.\*



# Does my Data leave EU boundary?

[Microsoft Cloud enables customers to keep all personal data within European Data Boundary - EU Policy Blog](#)



## EU Data Boundary

[Microsoft EU Data Boundary Overview | Microsoft Trust Center](#)



## Data Movement

[Enable copilots and generative AI features - Power Platform | Microsoft Learn](#)



## Intellectual Property

[Introducing the Microsoft Copilot Copyright Commitment](#)



## Supplemental Terms

[Legal Docs | Microsoft Dynamics 365](#)



## Privacy Statement

[Microsoft Privacy Statement – Microsoft privacy](#)



## Services Agreement

[Microsoft Services Agreement](#)

# AI transformation imperatives



Unlock productivity across your business with Copilot in Power Platform



Build transformational AI solutions with Microsoft Azure



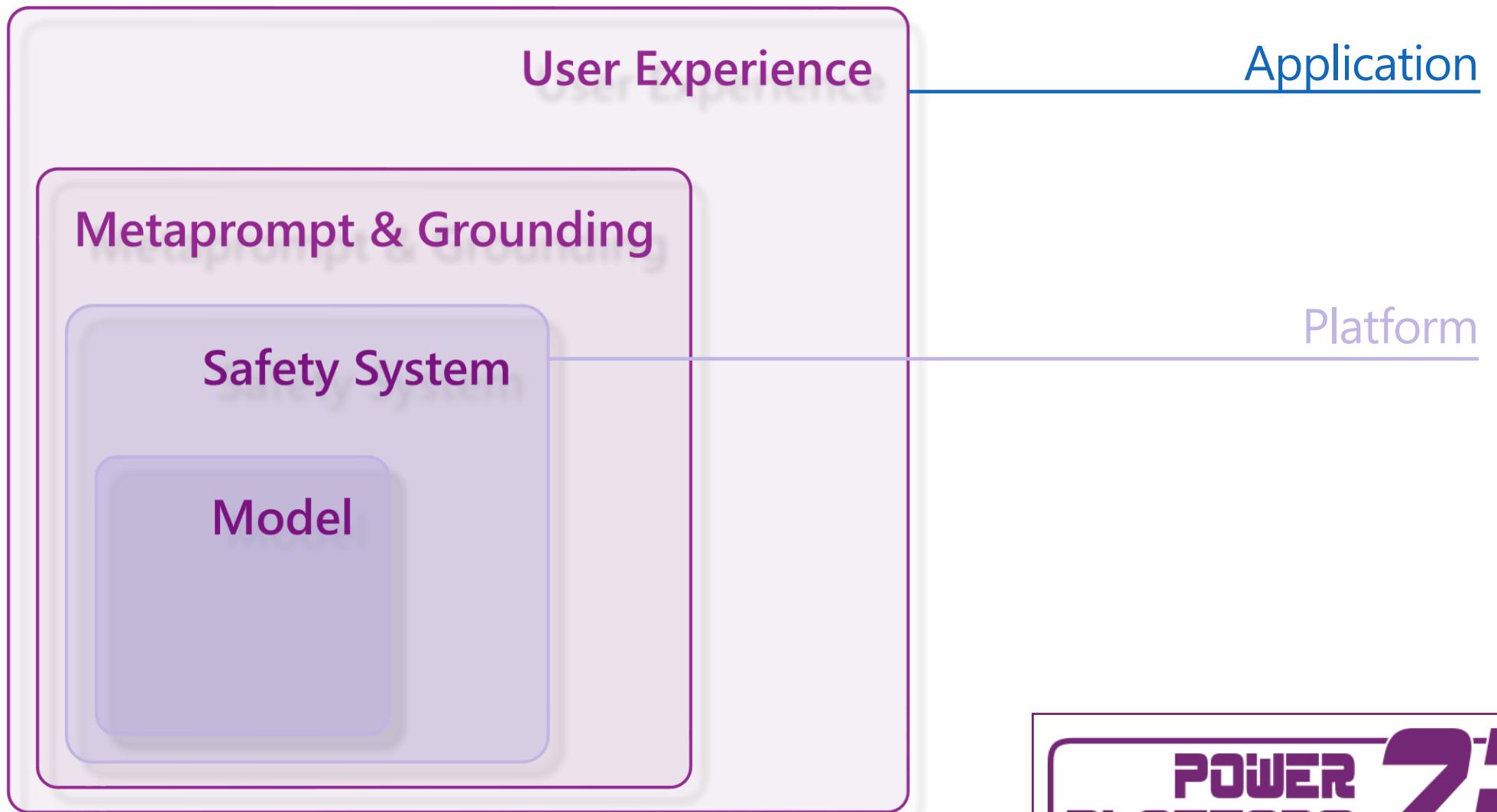
Co-innovate with trust and safeguard your business

eXalent<sup>s</sup>

**365**  
training

POWER  
PLATFORM 24

# Mitigation Layers



## Create an app

Edit table properties

## Client Meetings

# Demo Time

Client Name	Project Goals	Mission Statement	Scheduled ...
John Doe	Increase sales by 10%	Provide excellent customer service	1/1/2022
Jane Smith	Launch new product	Become a market leader	2/15/2022
David Johnson	Improve website performance	Enhance user experience	3/30/2022
Emily Brown	Expand into new markets	Build strong partnerships	4/15/2022
Michael Wilson	Optimize supply chain	Reduce costs and improve efficien...	5/31/2022

Copilot



Build a responsive mobile application for tracking client meetings, including the project goals, mission statement, and scheduled completion date. Generate some demo data for presentation.

Here is a table for tracking client meetings

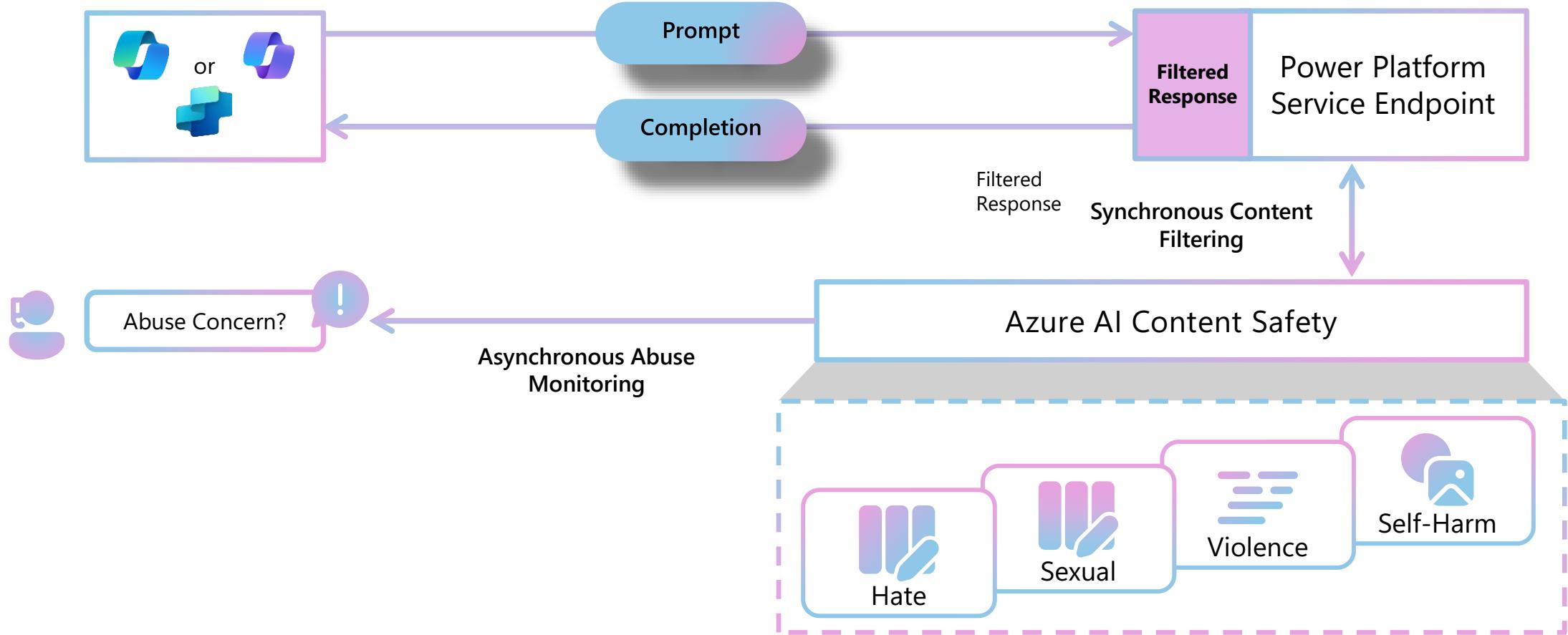
AI-generated content may be incorrect



add demo data from /MyExcelFile.xlsx

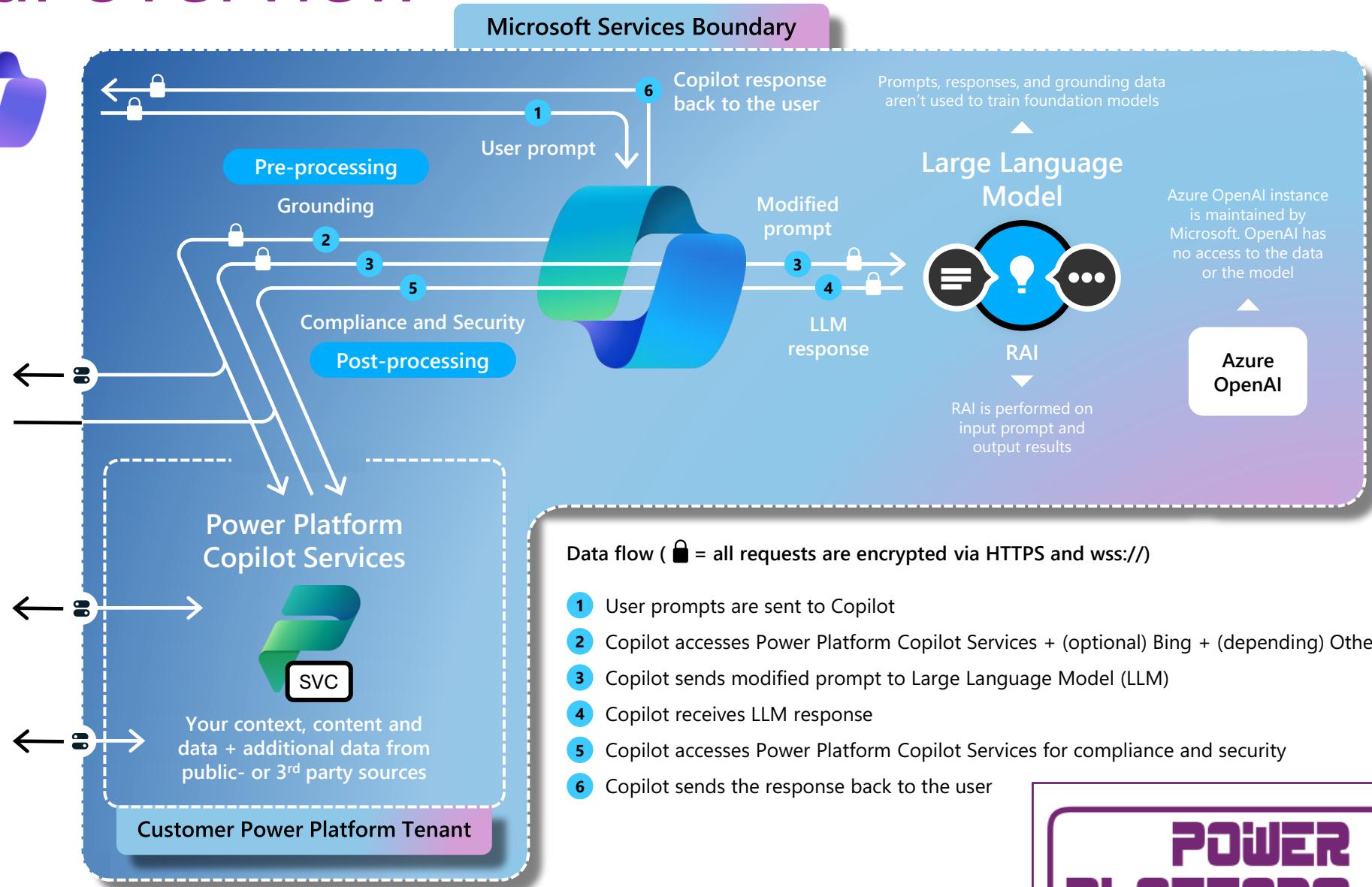
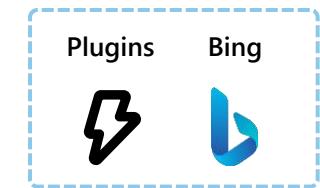


# Deploy foundation models with built-in safety system



Given the existing control layers and to avoid further logging of customer data, Azure OpenAI abuse monitoring is disabled for Copilot Studio generative AI features

# General overview



# Retrieval Augmented Generation

Each Copilot Service finds grounding data

We don't "train" on your tenant data



User prompt + Grounding data + Chat history + System prompt

Response + (optional) App command



# How does Copilot „drive“ a Power Platform app – (app commands)

Abstraction and compact footprint

Constrained to safe actions

Extendable to leveraging internal APIs

Auto-recover from errors

## LLMs

Natural language understanding

Implement text-to-text transforms

Great at text-to-code

## Program Synthesis



```
// Program to insert new screen with containers for responsible design  
// and selected Theme for applying properties  
  
# Get user selected screen  
screen = app.selected_screen()  
  
# Select new default theme  
theme = user.selected_theme()  
  
# Insert new screen based on LLM response  
new_screen(screen_name, containers, theme, mode)
```

## Transpilation



## Programmatic Power Platform APIs &

## Interpreter

Encode application-specific domain knowledge

Implement text-to-action transforms  
(i.e., can fulfill user intent)

extends

**365**  
training

**POWER**  
**PLATFORM** **24**

# Prepare for the era of AI



Goals



Pain points



Current  
capabilities



Data strategy



Resource and  
adoption readiness

# Thank You!



Thank you to all of our presenters and attendees!

Special thanks to **365<sup>o</sup>training** for hosting the live event and recordings!

Thanks to **eXalents** for helping us organize today's event

**eXalents**

**365<sup>o</sup>  
training**