# Risk Assessment for Copilots in Power Platform

Carsten Groth

20 March 2024


eXalents

365 DOT training

# 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

# 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

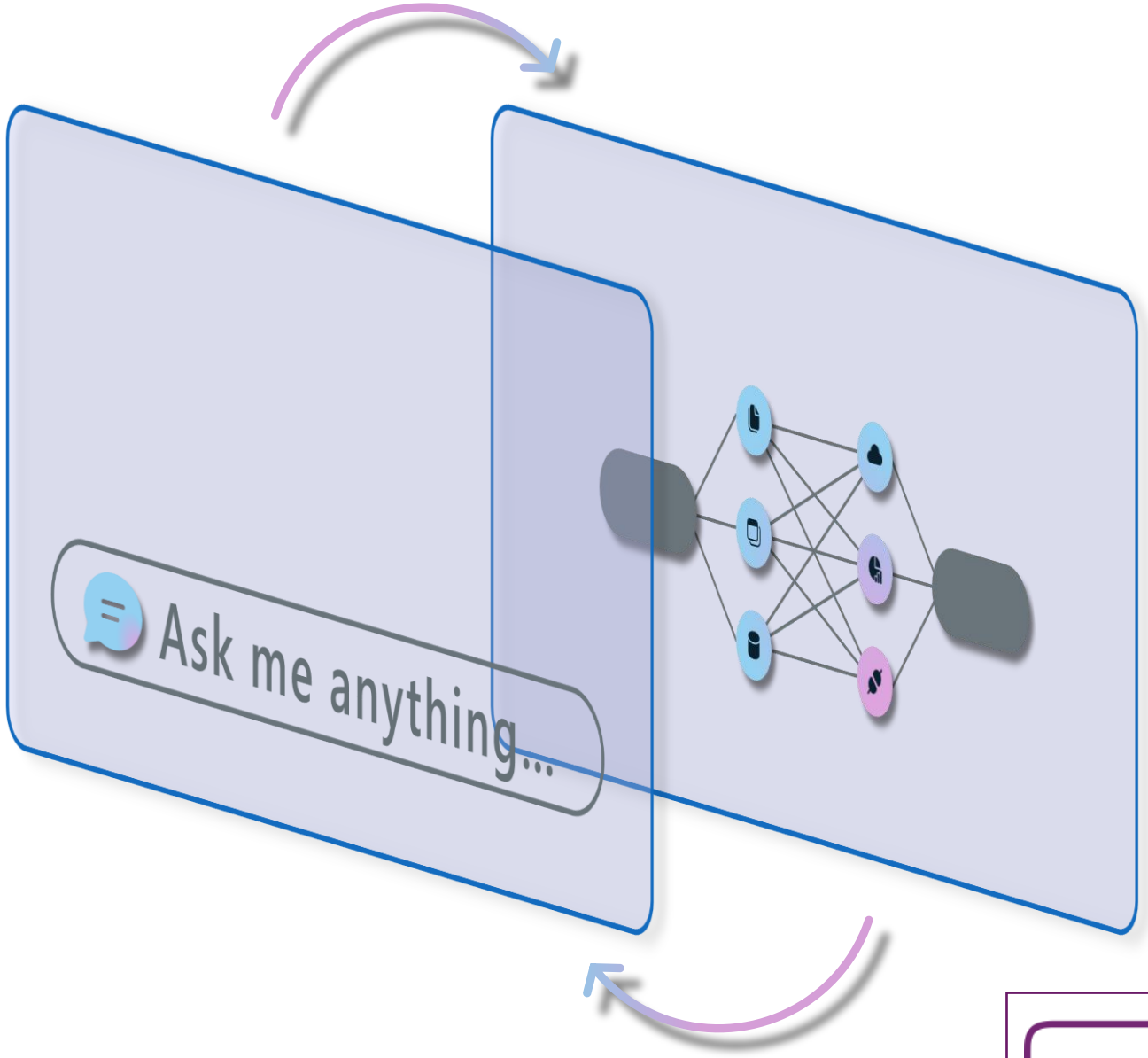
Copilot to assist with product-related questions

eXalents

365 DOT training

PLATFORM 4

Natural user interface



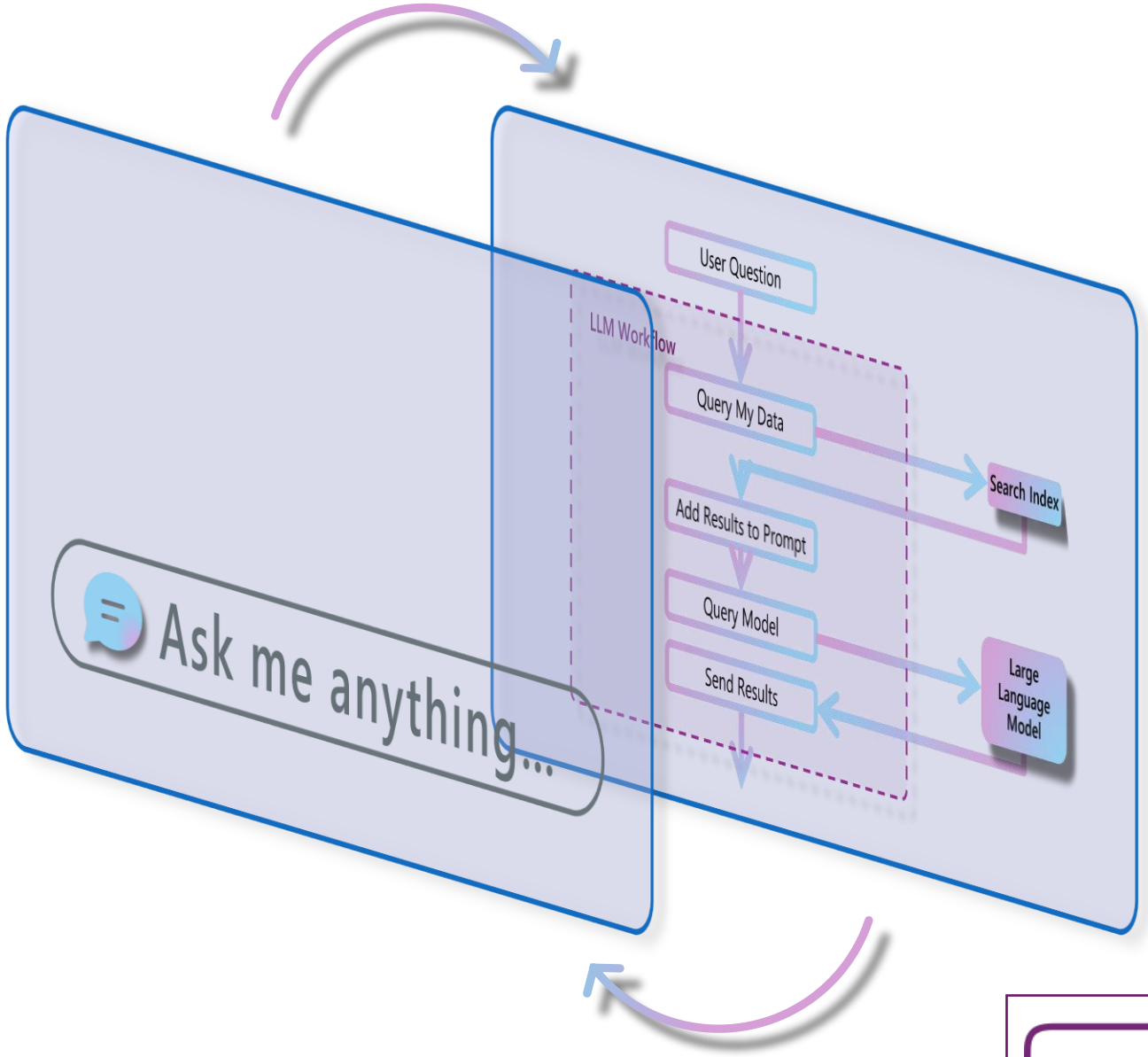

Reasoning engine

eXalents

365 DOT training

POWER PLATFORM 24

Natural
user interface

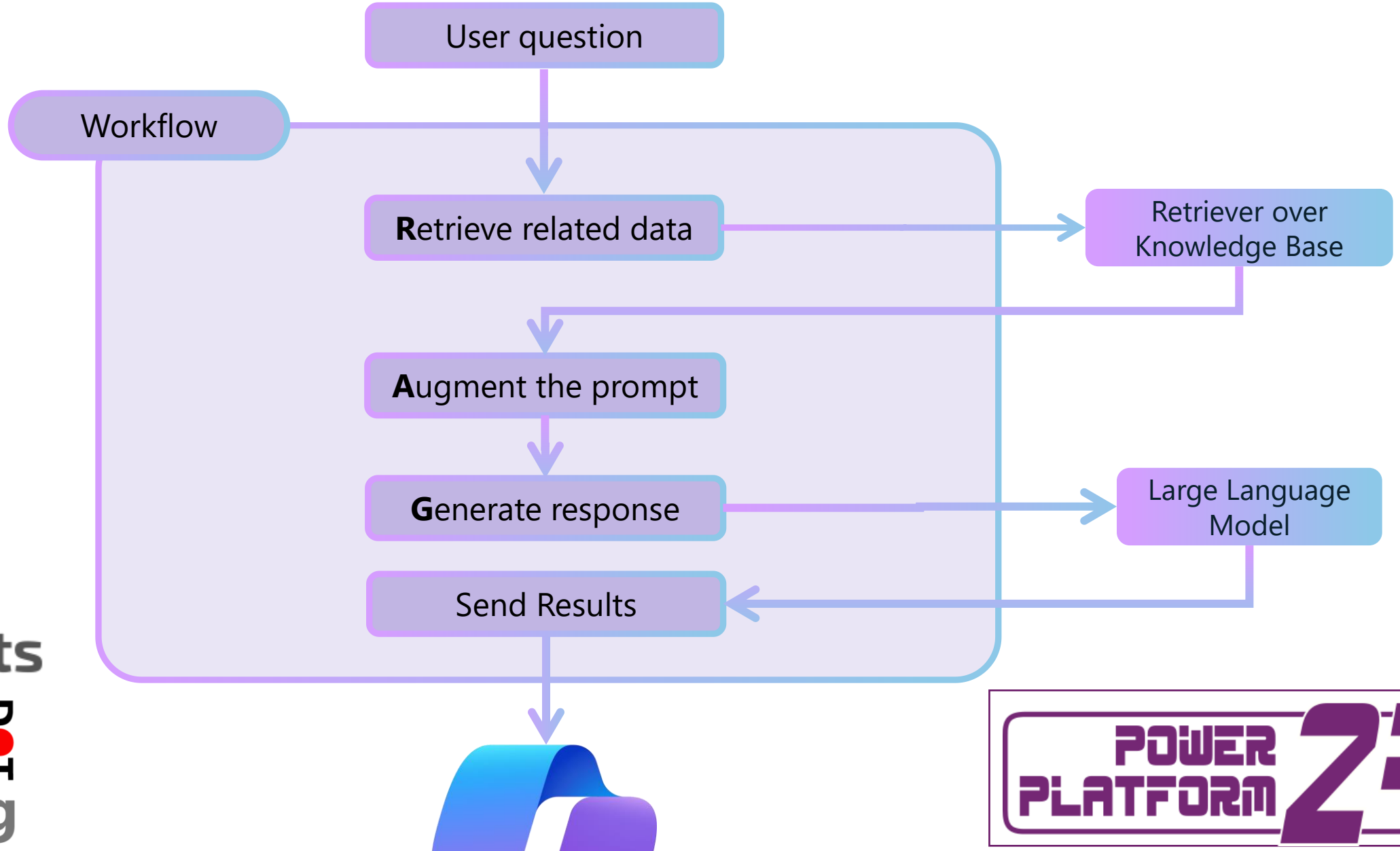



Retrieval
Augmented
Generation

eXalents
365 DT training

POWER PLATFORM 24

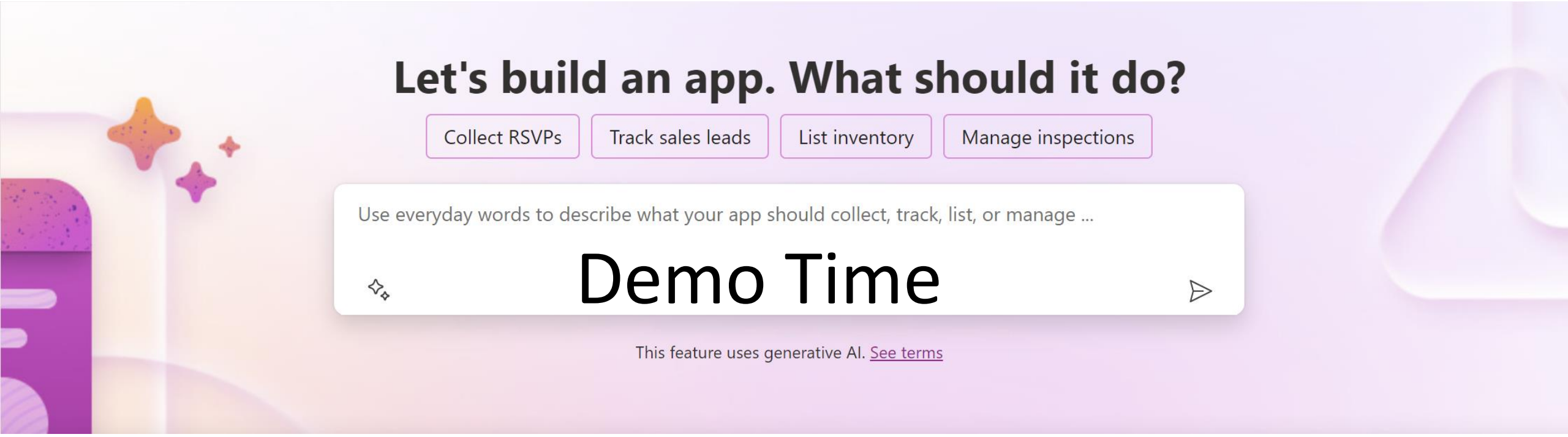
# Retrieval Augmented Generation (RAG)




eXalents

365 DOT training

POWER PLATFORM 24



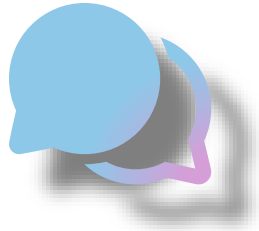

eXalents

365 DOT training

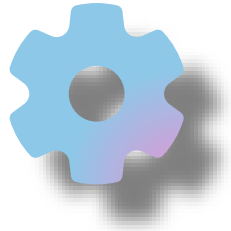
POWER PLATFORM 24

# 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.

# Evaluation matrix

**Groundedness**

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

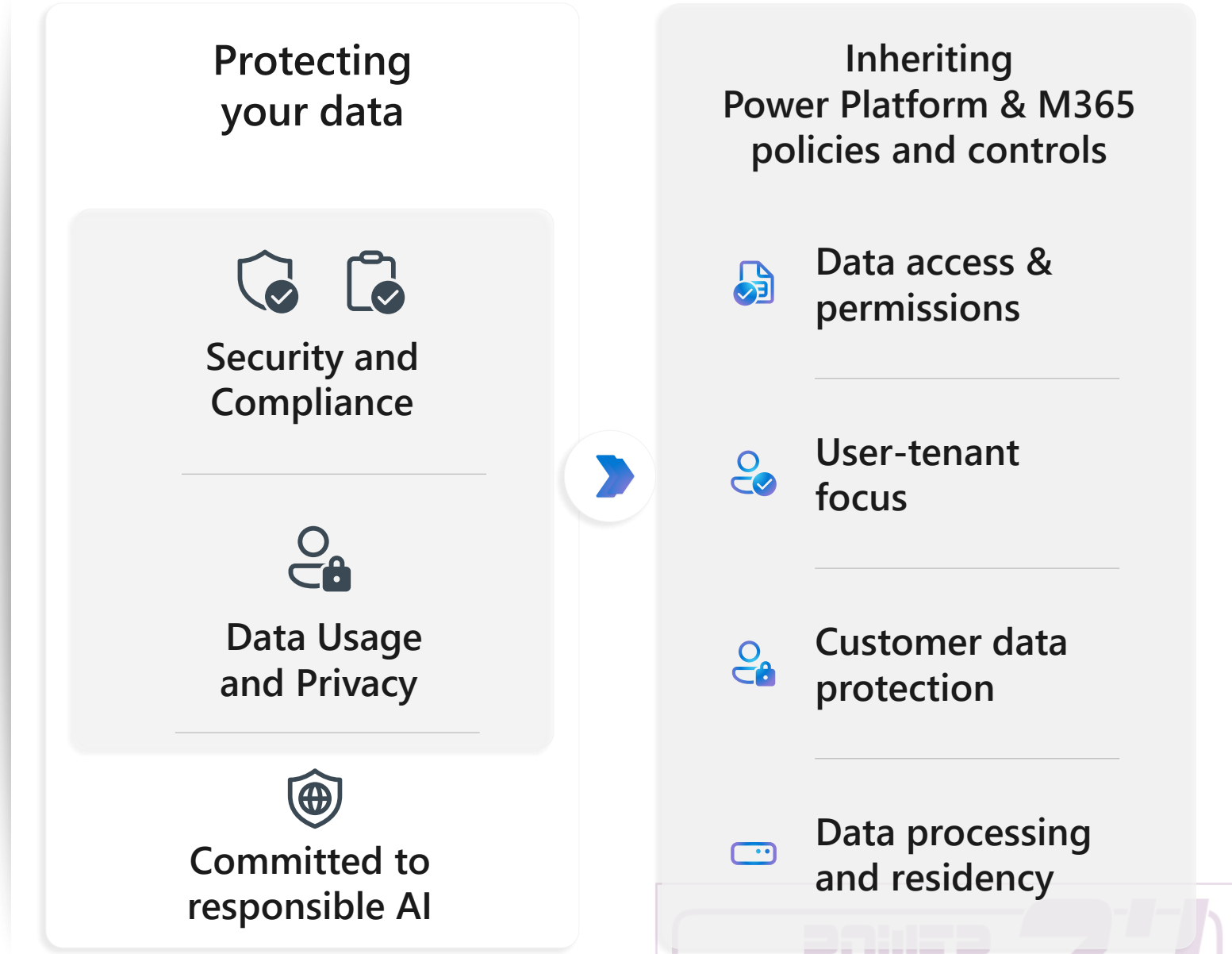
**Relevance**

Is the model's generated response relevant for given question

**Coherence**

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

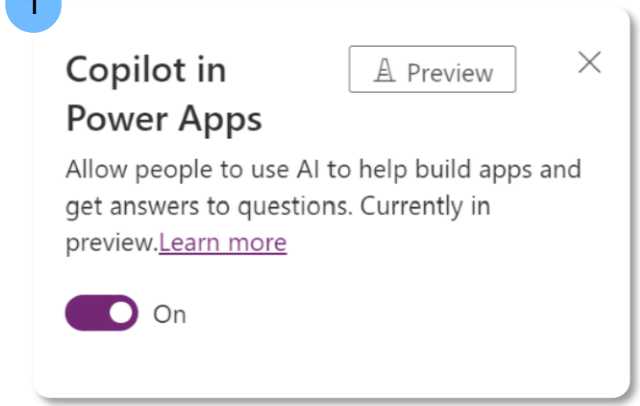
# Microsoft protects your data and enables you to control it



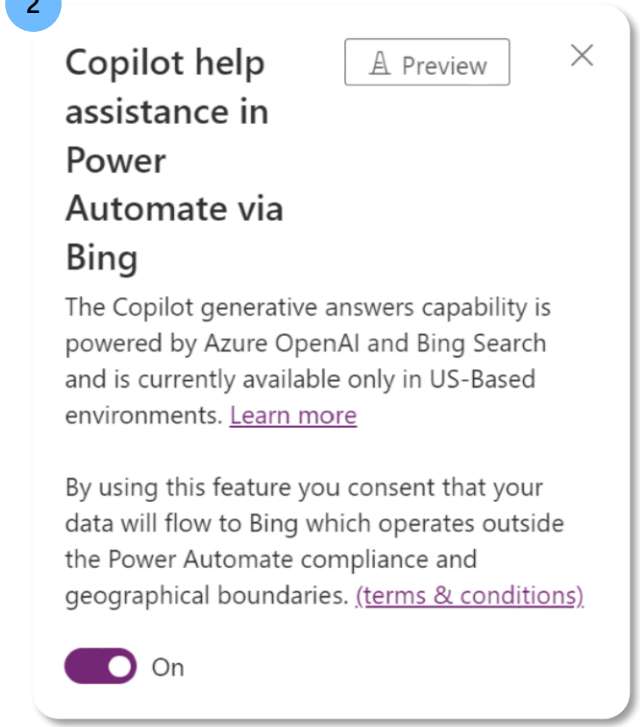
# Power Platform Copilot Governance (Tenant level)

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.

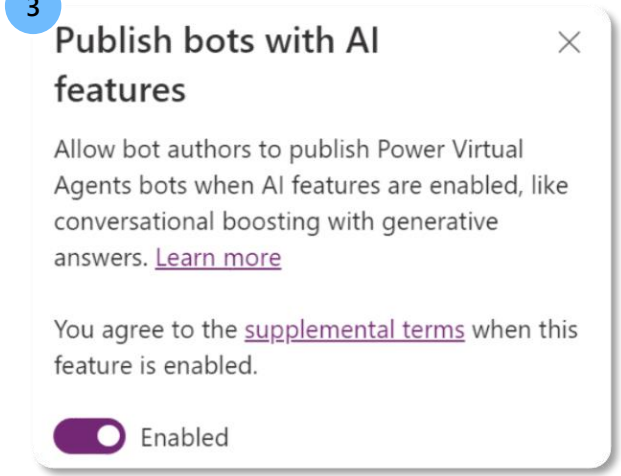
1



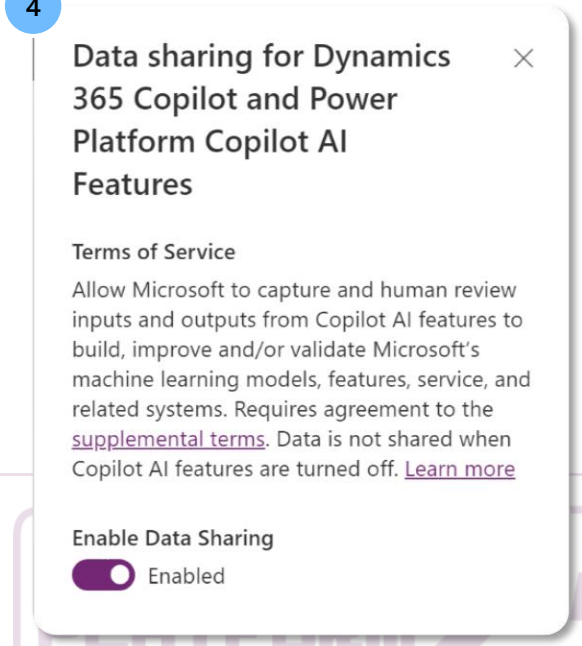

2




3

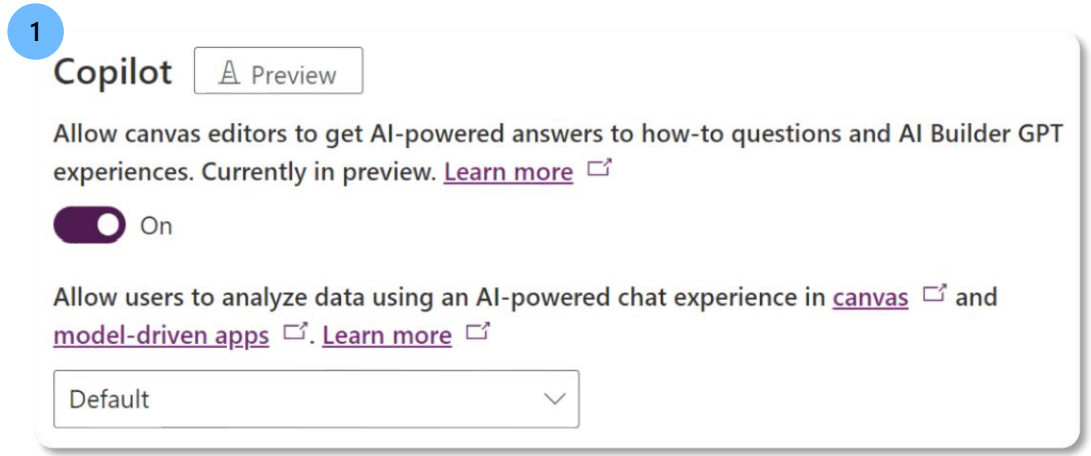


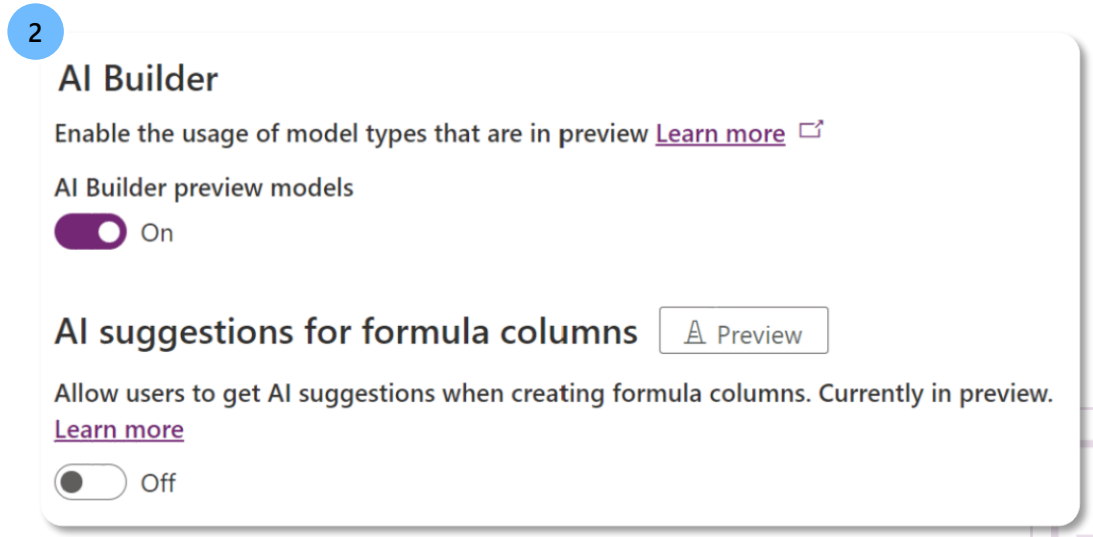

4

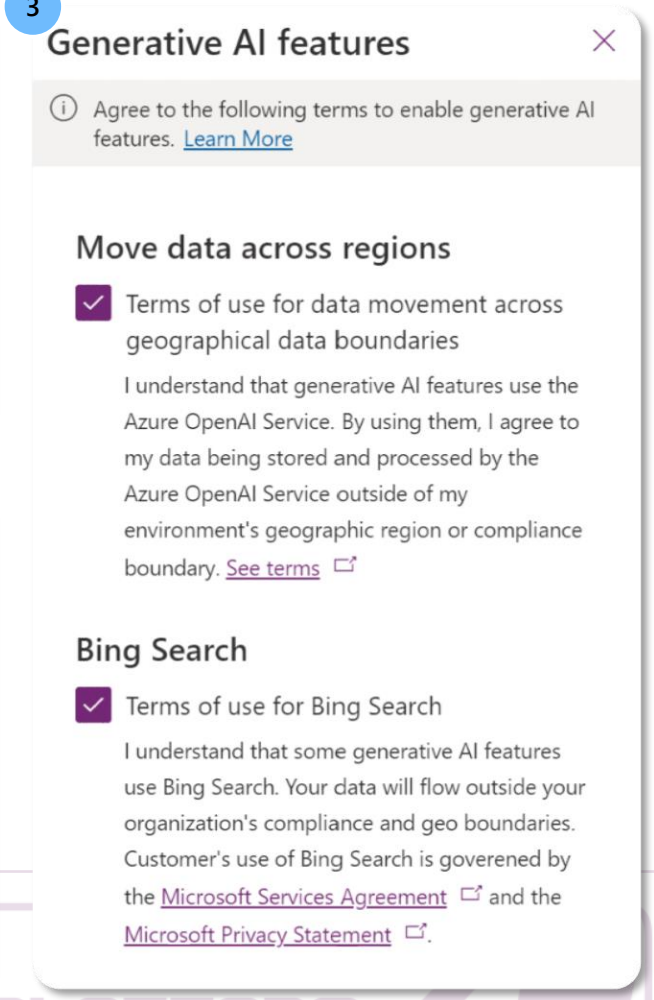


# Power Platform Copilot Governance (Environment level)

1. Control Copilot for canvas editors and Copilot chat experience for end-user
2. Control AI Builder models and using AI in formula columns
3. Opt-in on access of Copilot for each environment when outside US, UK, and Australia



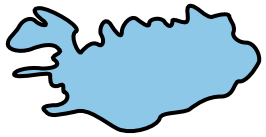
# Potential harms with generative AI

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

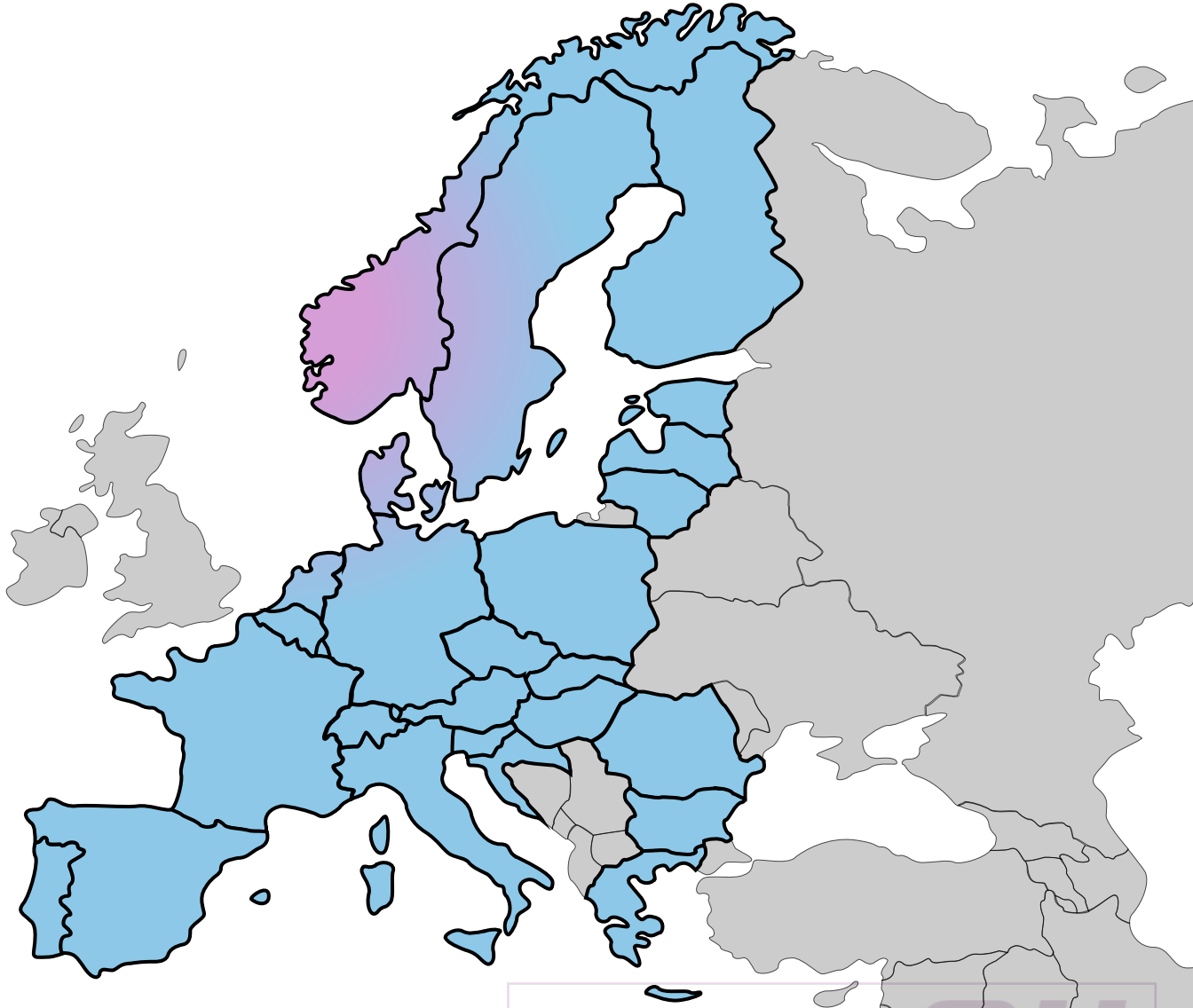
# Microsoft enterprise AI safeguard

- 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

# 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.*



eXalents 365 DOT training

*NOTE: Some services are temporarily or permanently exempted from this boundary. Specific exemptions are listed on Microsoft Learn.

# 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

### Supplemental Terms

Legal Docs | Microsoft Dynamics 365

### Data Movement

Enable copilots and generative AI features - Power Platform | Microsoft Learn

### Privacy Statement

Microsoft Privacy Statement – Microsoft privacy

### Intellectual Property

Introducing the Microsoft Copilot Copyright Commitment

### Services Agreement

Microsoft Services Agreement

eXalents 365 DOT training

# AI transformation imperatives

Unlock productivity across your business with Copilot in Power Platform

Build transformational AI solutions with Microsoft Azure

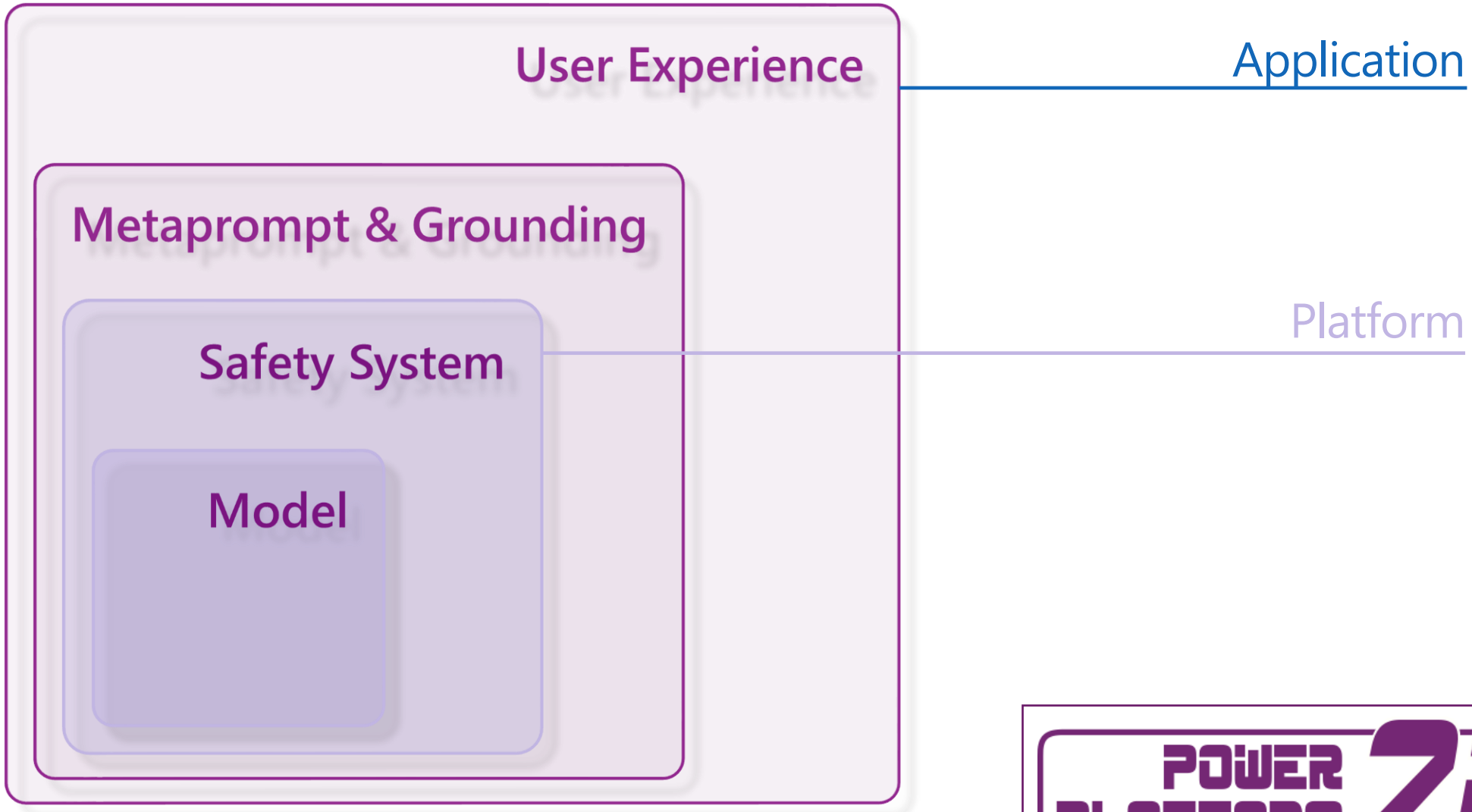
Co-innovate with trust and safeguard your business

eXalents

365 DOT training

POWER PLATFORM 24

# Mitigation Layers



# Create an app

Edit table properties

# Demo Time

## Client Meetings

| 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.

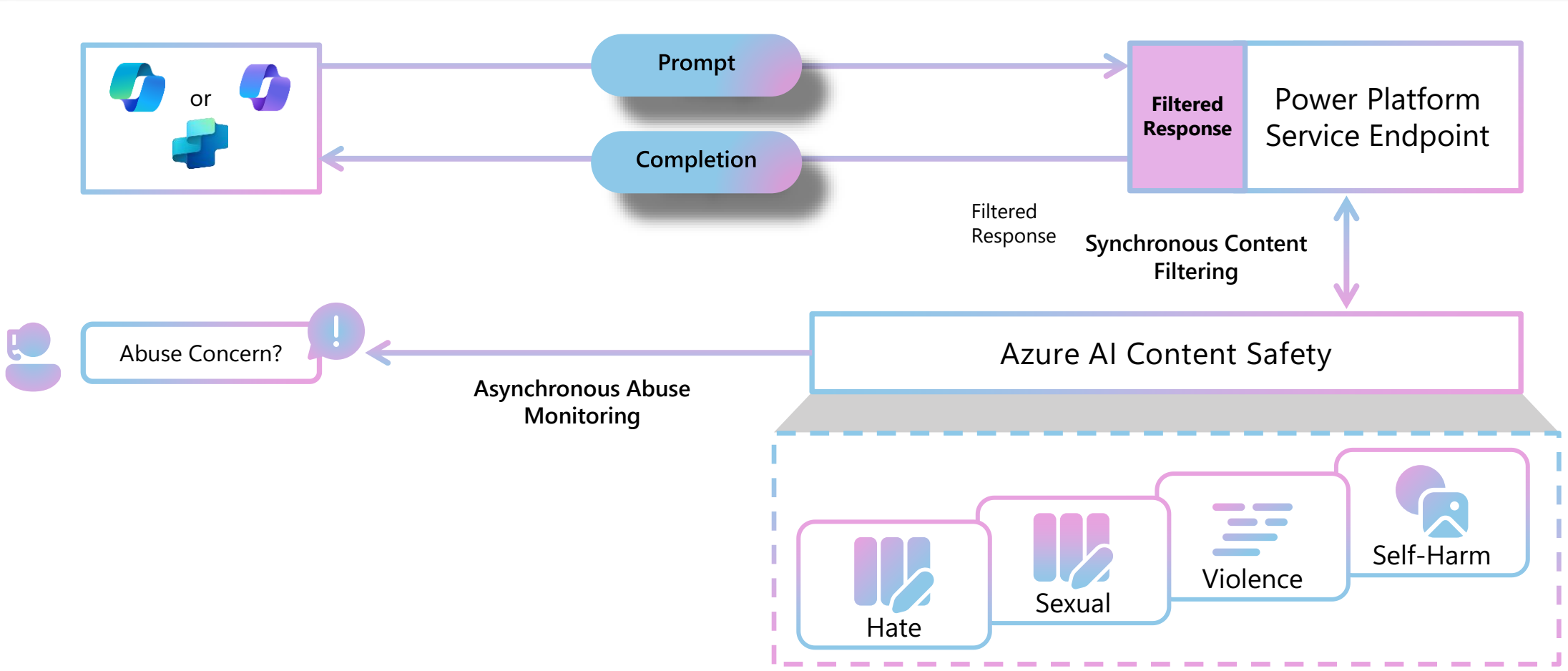
Here is a table for tracking client meetings

AI-generated content may be incorrect

add demo data from /MyExcelFile.xlsx

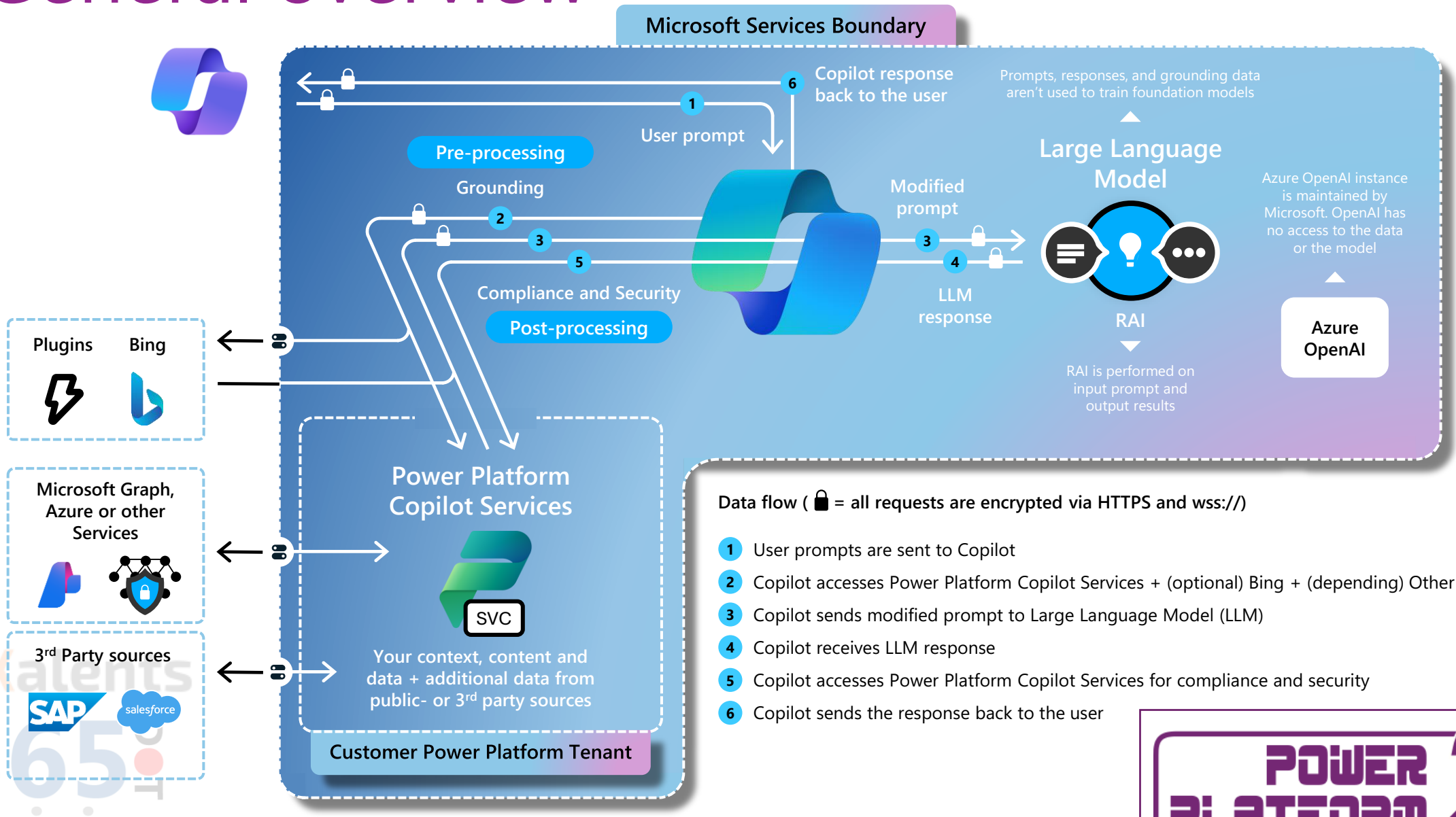
Make sure AI-generated content is accurate and appropriate before you use it. See terms

# 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



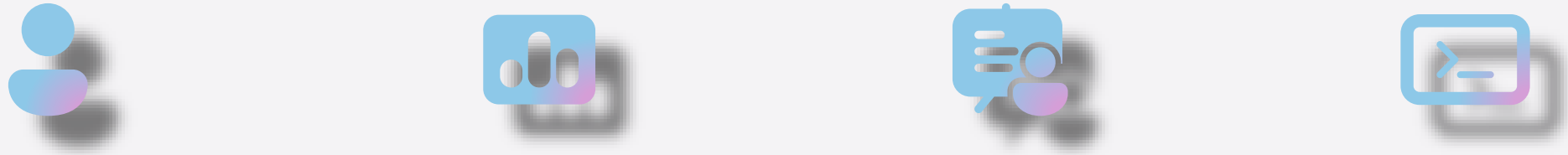

**Data flow ( 🔒 = all requests are encrypted via HTTPS and wss://)**

1. User prompts are sent to Copilot
2. Copilot accesses Power Platform Copilot Services + (optional) Bing + (depending) Other services for grounding
3. Copilot sends modified prompt to Large Language Model (LLM)
4. Copilot receives LLM response
5. Copilot accesses Power Platform Copilot Services for compliance and security
6. Copilot sends the response back to the user

# 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
- Extendable to leveraging internal APIs
- Constrained to safe actions
- 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)

# Prepare for the era of AI

# Thank You!


Thank you to all of our presenters and attendees!

Special thanks to 365 DOT training for hosting the live event and recordings!

Thanks to eXalents for helping us organize today's event

eXalents

365 DOT training