I want to become your companion – a different look at Copilot

Carsten Groth,
Chris Huntingford
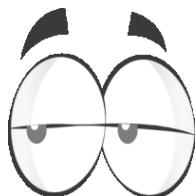
LAB 0: FLOORPLAN TO ESCAPE

Microsoft Services Boundary

Copilot response back to the user

User prompt

Pre-processing

Grounding

Modified prompt

Compliance and Security

Post-processing

LLM response

Large Language Model

Prompts, responses, and grounding data aren't used to train foundation models

Azure OpenAI instance is maintained by Microsoft. OpenAI has no access to the data or the model

RAI

RAI is performed on input prompt and output results

Azure OpenAI

Actions   Bing

Microsoft Graph, Azure or other Services

3rd Party sources

Power Platform Copilot Services

SVC

Your context, content and data + additional data from public- or 3rd party sources

Customer Power Platform Tenant

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

ColorCloud   www.colorcloud.rocks   #ColorCloud2024

Lab 1: M365 Copilot or Custom Copilot?

Customize
Copilot for Microsoft 365

Customize Copilot to work with your unique business processes and data sources

Configure Copilot responses to specific questions

Build a plugin

With Copilot Studio
(included in Copilot for M365)

Build your own
custom copilots

Enhance customer experiences by adding a copilot to your external website or other channels

Build an internal copilot outside of Microsoft Copilot to help employees with specific functions

Build with low code

With Copilot Studio
(standalone)

Customize Copilot for Microsoft 365 to…

Surface business data outside of Copilot
Connect Copilot to your business data and apps, such as CRM, ERP, and line-of-business apps.

Incorporate your processes
Easily customize Copilot to automate your business processes and workflows.

Configure how Copilot responds
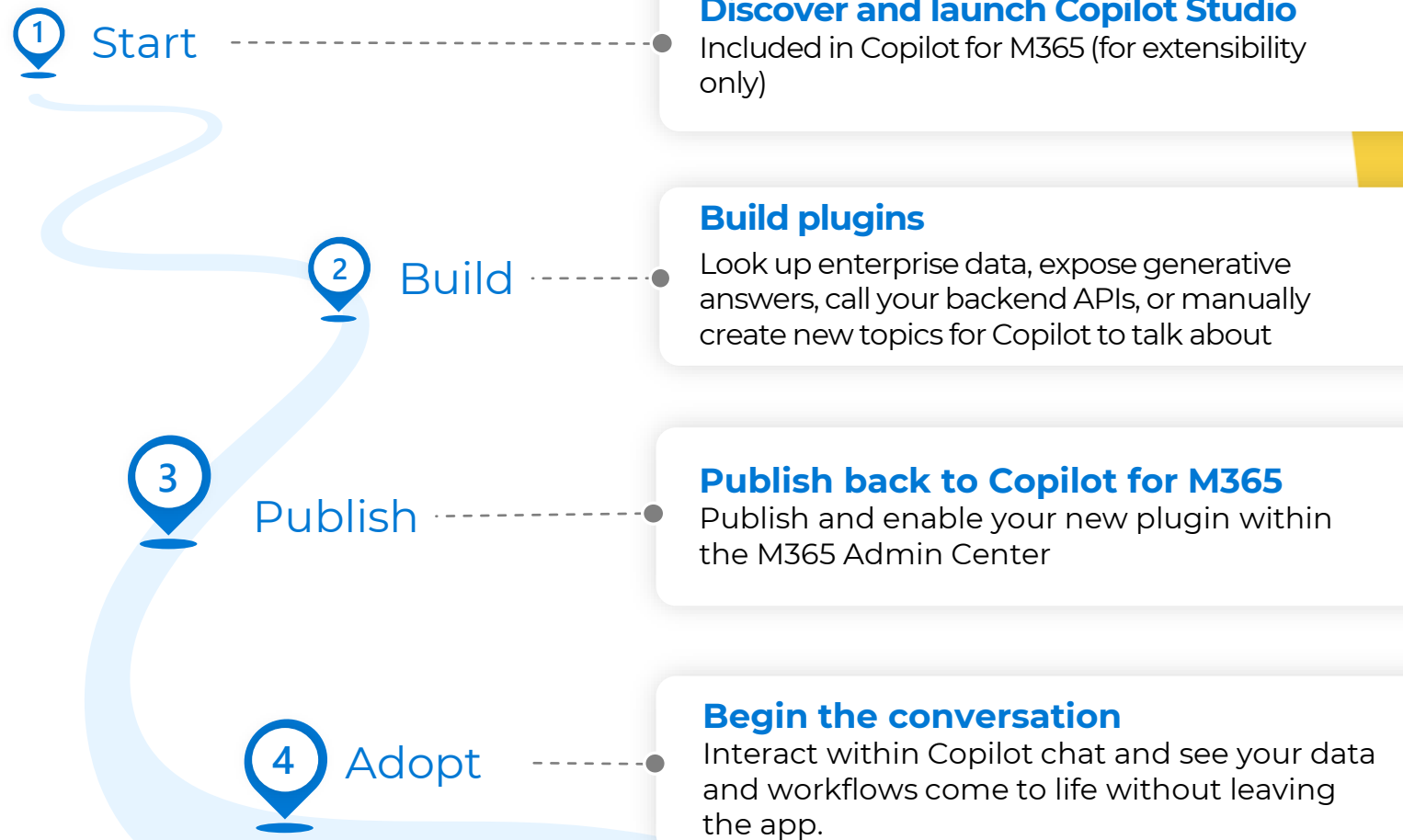Control how Copilot responds to specific questions with manually created topics.

Manage centrally
Secure your Copilot customizations with the right access, user controls, and analytics.

Create powerful custom copilots

Build and test together

Users of all skill levels can create automated, connected conversational AI experiences in one comprehensive platform.

Design personalized, responsive interactions

Engage employees or customers with rich, dynamic interactions that remember user content and context.

Boost your conversations

Use generative AI to dynamically respond using your organization's real-time content.

Handle complex queries with ease

Design intelligent conversations with greater control over the LLM such as robust variable and dialog management, logic, and responses.
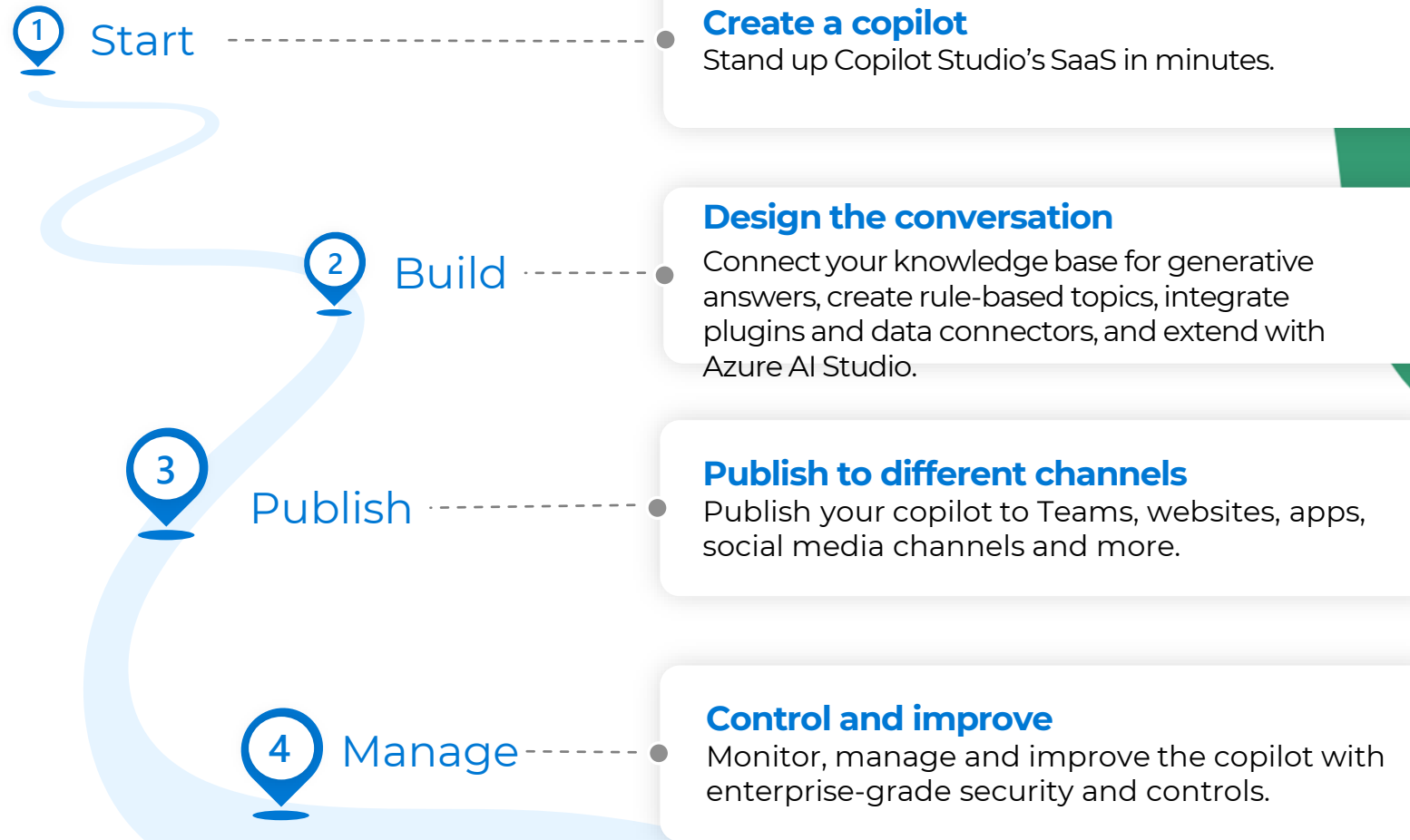
Continuous self-learning and improvement

AI-driven features will improve your copilot over time and provide suggestions on how to optimize your conversations.

How to build a custom copilot

1 Start

Create a copilot
Stand up Copilot Studio's SaaS in minutes.

2 Build

Design the conversation
Connect your knowledge base for generative answers, create rule-based topics, integrate plugins and data connectors, and extend with Azure AI Studio.

3 Publish

Publish to different channels
Publish your copilot to Teams, websites, apps, social media channels and more.

4 Manage

Control and improve
Monitor, manage and improve the copilot with enterprise-grade security and controls.

LAB 2: THE „RAG" IN COPILOTS

RETRIEVAL AUGMENTED GENERATION (RAG)

User prompt + Grounding data + Chat history + System prompt
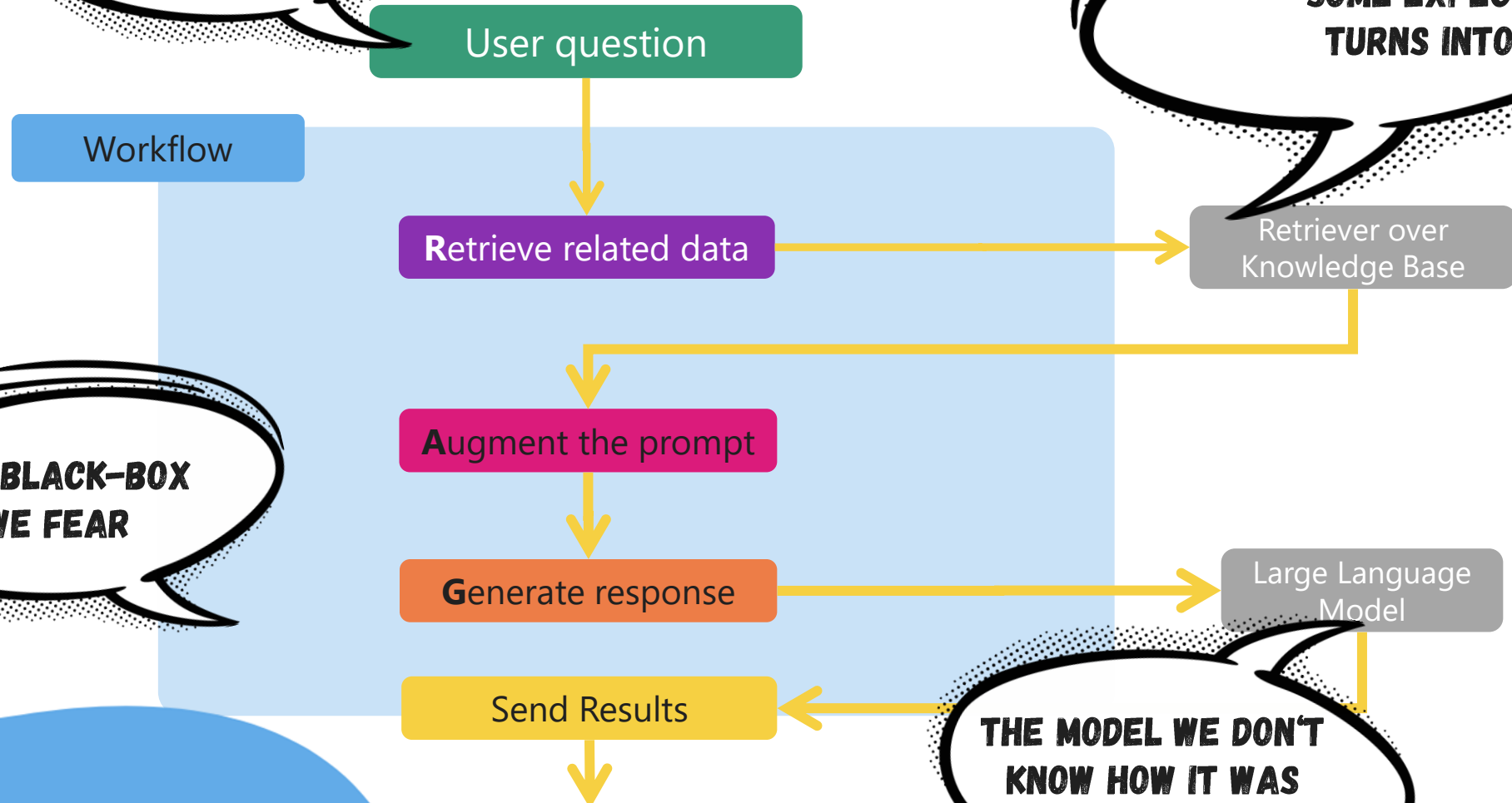
LAB 3: WHAT ABOUT YOUR DATA?

- Do you have concern your data leaving EU data boundary?
- Do you have concern about sensitive data being leaked through user prompts?
- Are you facing any legal compliance issues?
- Do you foresee any prompt injection attacks?
- Are you scared about any human-like behavior?

User Experience

Metaprompt & Grounding

Safety System

Model

Application

Platform
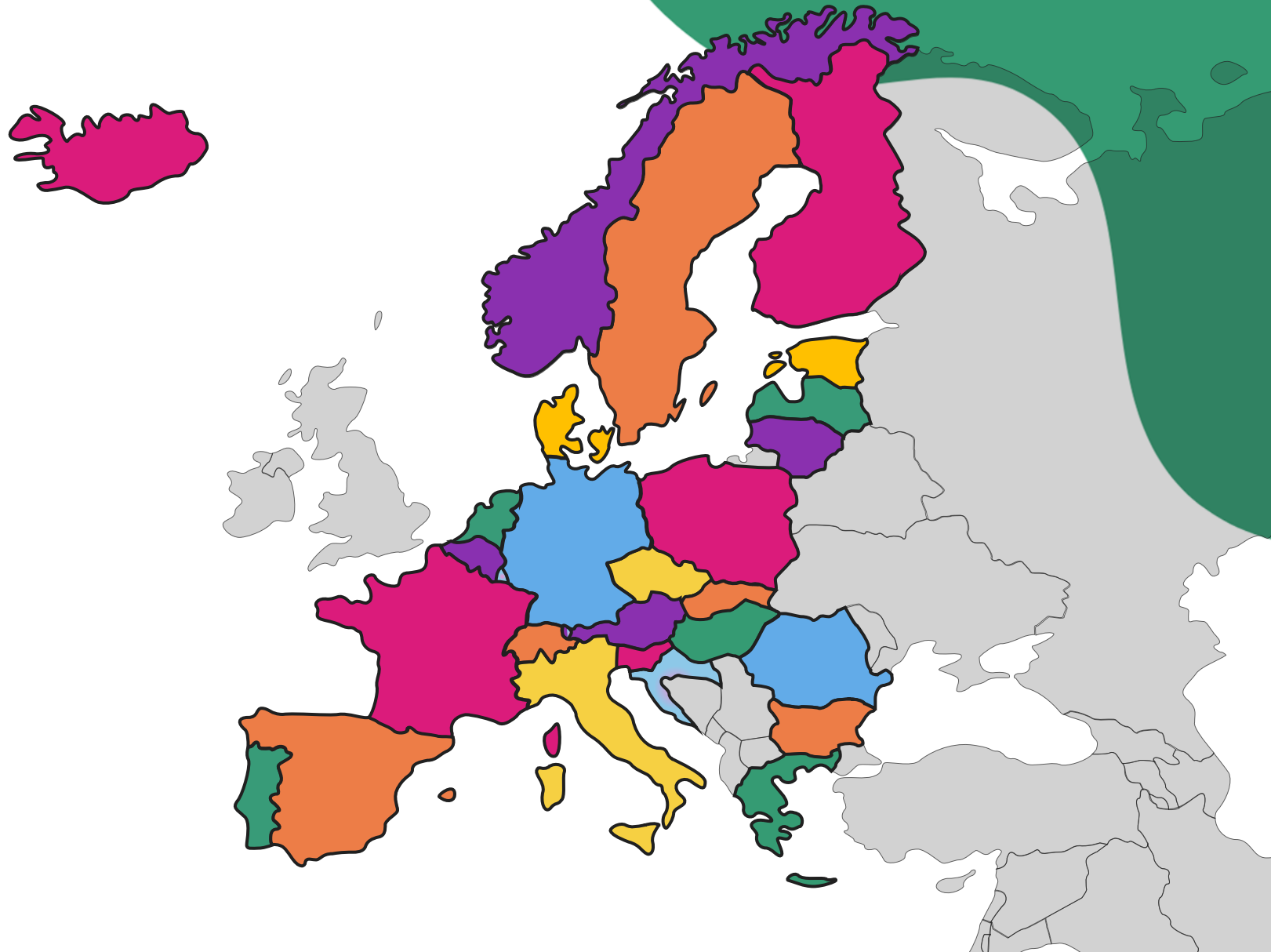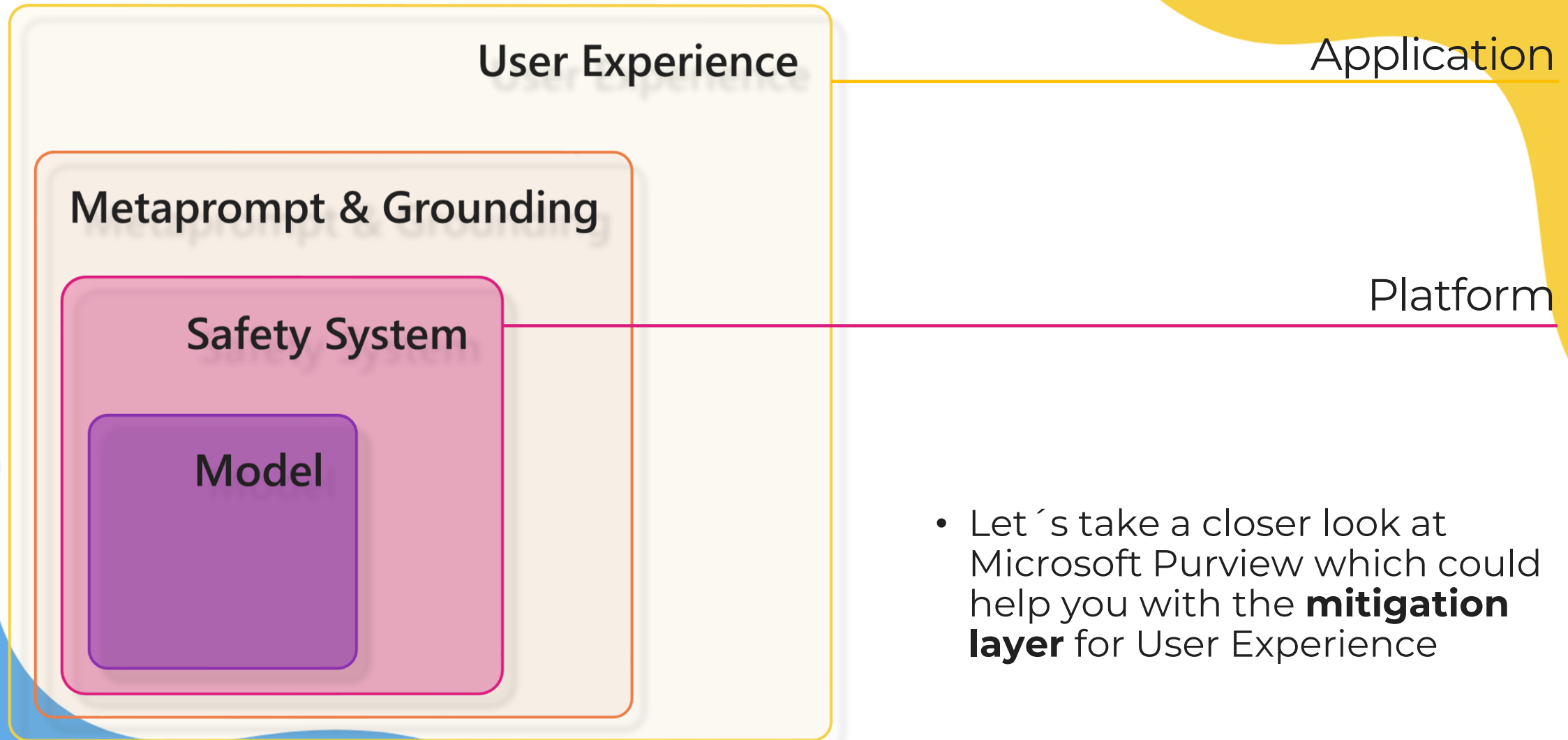
- Let´s take a closer look at Microsoft Purview which could help you with the **mitigation layer** for User Experience

ColorCloud   www.colorcloud.rocks   #ColorCloud2024

WRAP UP: THE „RAG" IN COPILOTS

RAG AND THE IMPORTANCE OF THE PROMPT

TASK

Provide an **instruction** telling the LLM what to be performed

CONTEXT

Describe the **data** that will be acted on, along with any input **variables**

CREATE A PRODUCT FEEDBACK SUMMARY BASED ON RECENT CUSTOMER REVIEW FOUND AT /___. THE SUMMARY SHOULD IDENTIFY KEY THEMES, OVERALL SENTIMENT, AND ANY RECURRING ISSUES OR PRAISES. FORMAT THE SUMMARY TO BE CONCISE, AND PRESENT THE INFORMATION IN CLEAR, EASY-TO-UNDERSTAND MANNER SUITABLE FOR A SELLERS TEAM MEETING

Convey to LLM **goals** and **expectations** on the response

Help LLM to format the **output** the way you´d like it to be

EXPECTATIONS

OUTPUT

Which tool for the job?

Software as a Service (SaaS)
No infrastructure to manage and built in security and governance

Platform as a Service (PaaS)
Manage own infrastructure, custom dev and security

Copilot Studio

+ Included in Copilot for M365	**Standalone**	**Azure AI Studio**
Customize Copilot for M365	**Build your own custom copilots**	
Connect with your data sources outside of Copilots reach	Build customer or internal facing copilots with your data and workflows, on channels that work for you	
Call your redesigned business processes and workflows	Rules-based dialog management and conversational orchestration with a prebuilt LLM	Configure LLMs with prompt engineering
Configure Copilot responses to specific questions	Managed SaaS, no infrastructure, built in security and governance	Manage own infrastructure, custom dev and security
Build a plugin	**Build Conversational Orchestration**	**Build Models**

Extend Copilot Studio with Azure AI Studio

Key take aways

- Retrieval Augmented Generation or vectorized search index crawling?
- Extend Microsoft 365 Copilot vs. building a custom copilot
- The best tool to use might be a combo, not a single tool
- Familiarize with an AI enterprise strategy → Ana and Andrew Welch (13:30)

Helpful Links

Empowering responsible AI practices | Microsoft AI

Power Platform | Copilot Risk Assessment | The Power Platform Talks (wordpress.com)

Copilot Studio – Education Series

Copilot Studio – Implementation Guide

Link to ANS Group Blog article