LLM: Retrieval-Augmented Generation.

Example: Microsoft with OpenAI

Prompt

"Customer Data" as per the DPA

Orchestrator App

2

4

1

3

Azure Cognitive Search

Knowledge Base

"Customer Data"

Azure Open AI Services*

LLM

5

Filtering App

7

Completion

"Customer Data" as per the DPA?

6

6

MS Operator (Default)**

Azure

Customer Operator*

1. The user enters request
2. The orchestrator app asks the LLM what it should query from the knowledge base (KB)
3. The orchestrator app obtains the information from the KB
4. The original request/prompt is expanded to include this KB information and again sent to the LLM for completion
5. The LLM completion is reported to Microsoft's filtering app for ethics & compliance checking
6. If necessary, the completion is checked manually
7. The completion is played out

| From/for Customer |
| From Microsoft |

→ Use of Azure within the framework of the existing contract conditions

Info: https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy

* The LLM does not store Customer Data and does not use it for its training.

** Customer may be able to opt out of Microsoft's ethis & compliance verification of the completion (and do it itself using Microsoft's monitoring tools, if necessary).

VISCHER
SWISS LAW AND TAX