FAQ meant for internal teams and (future) official documentation

Common FAQ – LLMs and Data Management

What agreements does UiPath have with 3rd party LLMs for Generative AI features?	UiPath has standard agreements with all third party sub-processor vendors which are assessed by our privacy and security teams to protect the governance and integrity of customer data.
Is my data being used to train 3rd party LLMs?	No, UiPath has agreements with all of its 3rd party processors – including LLM providers – to not allow customer data passed through the UiPath platform to be used for general model training. Find additional details on our UiPath Trust and Security site.
Where are my data being sent or used with 3rd party LLMs?	Any data that is used as context for prompts will be securely sent by UiPath only to 3rd party LLMs in the UiPath trusted ecosystem. UiPath has standard agreements in place with 3rd party LLMs and other model processors to not retain, use for training, or share customer data. Find additional details on our UiPath Trust and Security site.
How does UiPath handle Personal Identifiable Information (PII) in my data?	It is the responsibility of UiPath customers to carefully manage the input of sensitive data including PII into UiPath products which may leverage 3rd party products or services (including LLMs) , however UiPath agreements with 3rd party LLM providers prevents the storage and retention of any data.. UiPath treats all customer data with the highest enterprise grade security and will help customers appropriately manage any reported PII that has been sent to UiPath.
Which models are my data being sent to?	UiPath discloses a list of all 3rd party processors in its sub-processor agreement. Find additional details on our UiPath Trust and Security site.
Where is my data being processed?	The location of UiPath software is disclosed in the Data Privacy Agreement; the location of 3rd party sub-processor data processing is disclosed in the UiPath sub-processor agreement. Find additional details on our UiPath Trust and Security site.
How can I control how users in my organization use our data with AI features?	UiPath recommends users leverage available resources and documentation to inform their decision for how best to use various AI features and products in the platform.
Can I use my own LLM for automation processes?	With UiPath Integration Service, you can leverage Generative AI connectors for Azure, Google, AWS, and others within your automation workflow. See the latest here. We will soon offer capabilities to allow customers to bring their own LLM tenant for specific generative AI runtime features.

Can I fine tune UiPath managed LLM or generative AI models?	UiPath does not provide tooling to support LLM or other generative AI model fine tuning.

LLM Gateway

How do UiPath generative AI features communicate with LLM models through the LLM Gateway (What is the communication protocol)?	UiPath features communicate through the LLM Gateway service to LLM Models using LLM Gateway service to the 3rd party LLM using REST APIs provided by the vendors over the HTTPS protocol
How is the LLM Gateway connected to a tenant?	The LLM Gateway is a service that runs in Automation Cloud, and like other services, has deployed scale units associated with a tenant for a given region
How is data sent securely to the LLM Gateway? How is it encrypted?	Data is encrypted using TLS 1.2 for data in transit, and AES 256 for data at rest. Read more here.
Do all AI features use the LLM Gateway?	Not currently, just for generative AI features; in the future, all AI model invocation from UiPath products will flow through the LLM Gateway.
What is the expected response times?	Response time for UiPath generative AI features largely depends on the UiPath feature availability, request token size, and capacity of the invoked LLM. This may be variable based on the model provider and version.

Data Governance

Data Retention	For generative AI features, how long is UiPath storing my data?	UiPath maintains a consistent approach to data storage for any products and services provided through the platform, as mentioned in the privacy policy and security documentation. UiPath will retain transactional data for generative AI features for up to 30 days, but may be deleted sooner upon customer request.
Data Storage	Where is data being stored?	Generative AI features will only store data related to the transaction between the automation and the generative AI feature on UiPath Automation Cloud servers. No customer data or automation transactional data will be stored or shared with UiPath 3rd party LLMs.

	How can we manage IP, sensitive data, and copyright when using generative AI for content creation?	UiPath will securely protect the integrity and privacy of any customer data sources connected to Automation Cloud. We recommend customers use discretion with the choice and access management for developers who may use these data for any automation, including those using generative AI features.
Data Transmission	Is my data encrypted?	All data used with UiPath products are treated the same; Data at rest is encrypted with AES 256, data in transit is encrypted using TLS 1.2. For additional details please see here.
	How can we control access to certain sources of data for users and generative AI models?	UiPath will support organization, tenant, and user group RBAC for all AI features and products, starting with generative AI.
Data Security	How does UiPath protect PII data?	UiPath will treat any customer PII with the highest scrutiny and security to protect the integrity of our customers, as is stated here. We will also detect any data shared with UiPath upon request. We will soon introduce new tooling for admins to specify the entities and mitigation of any PII that could be used with AI models – stay tuned!
	How do we protect the privacy of individuals in data used with generative AI?	If there is indiscriminate personal information within data used for generating predictions, customers may request UiPath to delete these data at any time.

Data Governance

What kinds of safeguards can be put in place to reduce mistakes or hallucinations from these models?	All UiPath AI products and features leverage a human in the loop to review and edit AI model predictions before they are used in downstream automation to reduce errors, ensure accuracy and consistent predictions.
How can we provide feedback to refine and improve Generative AI model responses?	UiPath will provide mechanisms to capture explicit user feedback and quality scores related to the LLM responses – stay tuned!
How can we prevent generative AI models from	Please ensure any prompts used with generative AI features are free from harmful or inappropriate content to prevent misinterpretation in the tone of response from the model. UiPath is partnering with a

generating harmful or inappropriate content?	number of AI model providers who are building safeguards into these LLMs to filter and prevent harmful content from reaching the models. UiPath encourages its users to leverage UiPath Academy and other resources to educate them on best practices for interacting with generative AI and other conversational AI models.
How can we mitigate bias that can be used to train/emerge from AI models?	Bias can occur in data as well as in the trainers who are training these AI models. To mitigate bias in data, UiPath encourages its customers to maintain a high level of scrutiny on the sources of data, content of data, and distribution of data types that are used by AI products and features. UiPath Generative AI features powered by 3rd-party vendor LLMs have standard opt-out agreements with UiPath to prevent any training of general models.
How do we establish transparency and explainability when using generative AI, especially in sensitive domains?	There are a variety of UiPath partners (AWS, H2O.ai, Google, etc.) who have Machine Learning Ops (MLOps) platforms that provide dashboards to track the traceability and interpretability of model predictions.
How can we monitor and audit generative AI model responses?	The UiPath LLM Gateway service will maintain and provide upon request telemetry data related to the invocation of generative AI prompts and responses.
What should be done to address the legal liabilities and responsibilities with the use of generative AI?	UiPath upholds a high standard of data security and compliance for all products. Before using generative AI features ensure a complete understanding of the UiPath platform, UiPath 3rd party sub-processors, and the UiPath product/feature to ensure the proper use of these tools.