OPAQUE

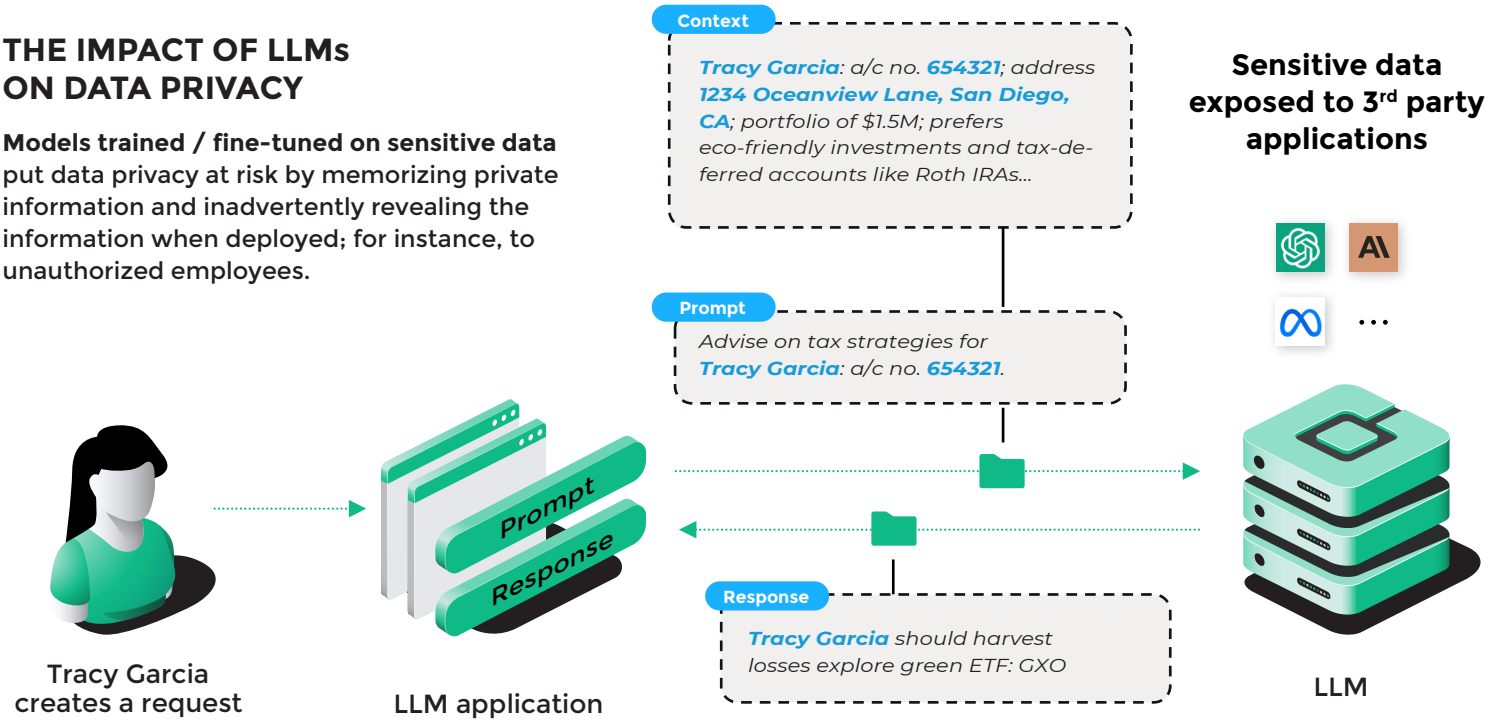
IN A RACE TO ADOPT GENAI AND PREVENT BEING DISRUPTED BY COMPETITORS, COMPANIES ARE CREATING UNPRECEDENTED RISK: **PRIVACY MATTERS MORE THAN EVER IN THE AGE OF GENERATIVE AI**

Generative AI and LLMs offer a groundbreaking opportunity to increase productivity and efficiency. Yet, without similarly innovative protective measures, the widespread use of generative models can threaten data privacy and leak sensitive company information.

Chief Information Security Officers (CISOs) identified the risk from insiders (27%) as the most challenging threat to pinpoint. A case in point is Samsung, whose employees accidentally leaked sensitive code by uploading it to ChatGPT.

THE IMPACT OF LLMs ON DATA PRIVACY

Models trained / fine-tuned on sensitive data put data privacy at risk by memorizing private information and inadvertently revealing the information when deployed; for instance, to unauthorized employees.



Using third party LLMs for AI applications (e.g. via chatbots) exposes the prompt and context data to the LLM provider, which can be very sensitive in nature – e.g. proprietary company data, or ***personally identifiable information (PII)***, as illustrated above.

BETWEEN SECURITY BREACHES AND EVOLVING PRIVACY REGULATIONS, BUSINESSES MUST ADOPT STRATEGIES TO PROTECT SENSITIVE DATA IF THEY WANT TO MAXIMIZE THE BENEFITS OF LLMs.

Organizations need a privacy-preserving AI solution that bridges the gap between protecting privacy and realizing the full potential of LLMs. To protect privacy throughout the stages of a generative AI lifecycle, strict data security techniques must be implemented to securely and efficiently perform all security-critical operations that directly touch a model and all confidential data used for training and inference.

OPAQUE

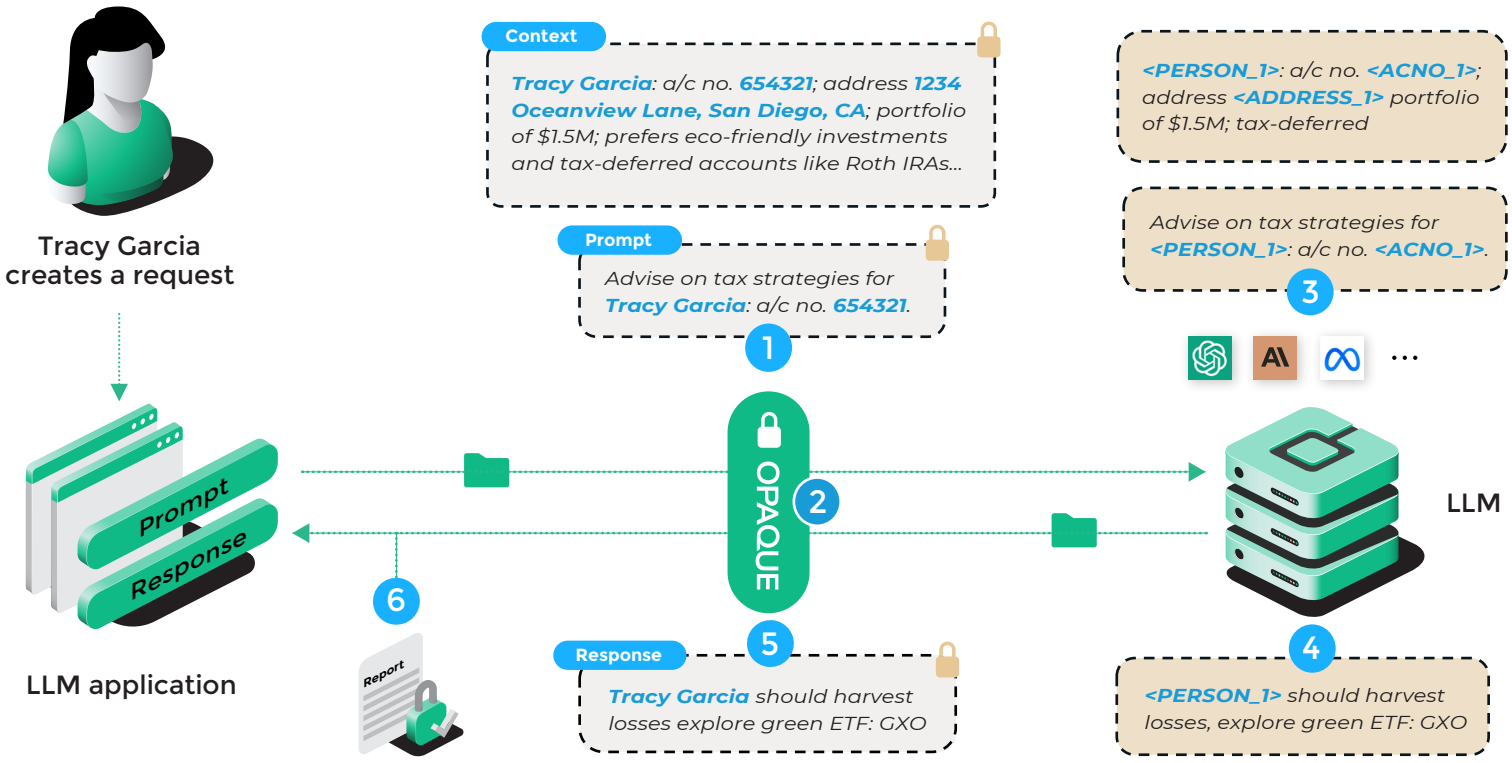
INTRODUCING OPAQUE GATEWAY:

PROTECT YOUR SENSITIVE DATA FROM MODEL PROVIDERS. LEVERAGE GENERATIVE AI AND LLMs, PRIVATELY.

Opaque Gateway serves as a privacy layer around your LLM of choice.

With Opaque Gateway, you can seamlessly sanitize LLM prompts to hide sensitive data from external parties and LLM providers.

Opaque's Confidential Computing technology ensures that no third party, not even Opaque Gateway, sees the underlying prompt.



HOW IT WORKS:

1. **Confidential Data:** The user prompt, including any context, is encrypted and sent to Opaque Gateway for processing. Sensitive information, such as personally identifiable information (PII) and proprietary data, is sanitized. Processing is configurable with client-provided dictionaries. The user, or their organization, manages the encryption key—privacy is provable and guaranteed.

2. **Prompt Compression,** AI Workloads, and Data Governance: Opaque Gateway uses prompt compression to minimize the data volume sent to LLM and reduce computational costs. Pre-existing guardrails and other AI workloads can be deployed to process encrypted data. It also includes advanced data governance features, which redact context data from RAG for different user groups, ensuring compliance with access controls and privacy regulations.

3. **Processing with LLMs:** During the pre-processing stage, data confidentiality is maintained using Opaque Gateway confidential computing. The sanitized and compressed prompt is then sent to the selected LLM, which can be swapped as costs and features evolve.

4. **The LLM produces a sanitized response** to the query. The sanitized data fields are not revealed to the LLM or the service provider.

5. **Post-Processing and Compliance:** After generating a response, the Opaque Gateway de-sanitizes it and returns it to the user application. Training data can also be cleaned up in the confidential gateway, ensuring data privacy and compliance.

6. **Monitoring, Reporting, and Proof of Compliance:** Opaque Gateway allows organizations to monitor and report on data handling throughout the process. An audit trail report, verified by signatures from CPU or GPU manufacturers, provides proof of compliance with data privacy regulations.