Bigtincan®

Artificial Intelligence Governance Charter

We understand that our customers have important questions regarding the security, fairness, and privacy of our AI-driven solutions. To address these, we've compiled a list of common inquiries about our AI practices and third-party integrations.

Here are some clear, detailed answers to ensure you are informed about how we approach AI, safeguard your data, and maintain ethical standards.

FAQs on Bigtincan's use of AI

01

Were the tools we use for our products tested for vulnerabilities?

The third-party LLM providers, such as OpenAI, perform their own security assessments, which typically include vulnerability testing as part of their development and deployment processes. The SaaS company relies on the security assurances and certifications provided by these third-party providers. Details on specific vulnerability tests would be best obtained directly from the third-party provider.

02

Were the tools tested for biases?

The third-party LLM providers actively research and implement techniques to mitigate bias in their models. However, it is important to note that while efforts are made to reduce bias, it is not possible to eliminate all biases entirely. The third-party providers typically release documentation and research papers that describe their approach to bias mitigation.

03

Describe the approach to test the data for bias which may be the result of different data limitations such as missing data, observational intensity, logistical limits, or low participation from different demographics.

The third-party LLM providers use a combination of data augmentation, diverse training datasets, and statistical techniques to test and mitigate biases that could arise from data limitations. These providers often publish their methodologies and research findings in technical documentation or academic papers, where they describe how they address issues like missing data, observational intensity, and demographic representation.

04

Define your bias/fairness testing methodology.

The bias and fairness testing methodologies employed by third-party LLM providers generally include:

- **Diverse Training Data**: Ensuring the training data includes a wide range of demographic groups.
- **Bias Detection Tools**: Using automated tools to detect and measure bias during the model development process.
- **Iterative Model Training**: Continuously refining models to reduce identified biases.

These methodologies are typically outlined in the third-party provider's public documentation.

05

Bias detection and fairness metrics should be pre-identified during the AI/ML Solution design phase to avoid the potential risk of erroneous or unguided measurement.

Third-party LLM providers often identify bias detection and fairness metrics early in the model design phase. These metrics guide the development and testing process to ensure the models perform fairly across different subgroups. The specifics of these metrics are generally included in the provider's technical documentation or research publications.

06

The pre-identified metrics should be used to repeatedly test and measure the AI/ML Solution performance across different subgroups applicable to the use case.

Third-party LLM providers typically use pre-identified metrics to test and measure model performance across various subgroups. This ongoing evaluation helps ensure that the models maintain fairness and reduce bias over time. Details on these metrics and their application are usually found in the provider's documentation.

07

How was the output evaluated for fairness, including unfair or harmful stereotypes? What were the results of the assessment?

Third-party LLM providers evaluate their models for fairness by analyzing the outputs for indications of unfair or harmful stereotypes. They use a combination of automated tools and human evaluations to identify and mitigate these issues. The results of these assessments are often summarized in the provider's documentation or research papers.

08

TLS scan results

TLS (Transport Layer Security) implementation details, including scan results, would typically be managed by the SaaS company if they handle the integration and data transport layers. For third-party LLM providers, TLS is generally part of their overall security infrastructure, and specific scan results would need to be obtained directly from them.

09

Vulnerability scan results

The SaaS company would rely on the third-party LLM providers' assurances regarding their vulnerability management processes. Specific vulnerability scan results for the LLMs would be proprietary to the third-party provider and are not typically disclosed publicly.

10

Process for confirming accuracy of output

The third-party LLM providers employ extensive validation processes to confirm the accuracy of their model outputs. These processes often include benchmark testing against industry standards, cross-validation techniques, and continuous refinement based on real-world feedback. The details of these processes are usually outlined in the provider's technical documentation.

11

Continuous Monitoring and Improvement: What processes do you have for continuously monitoring and improving the accuracy of your AI services?

Third-party LLM providers continuously monitor and improve the accuracy of their models through a combination of real-time performance tracking, periodic re-training with new data, and user feedback integration. They regularly update their models to adapt to new data and use cases. This process is typically described in the provider's documentation.

12

Has the AI feature or LLM undergone independent statistical validation for accuracy of its outputs?

Yes, many third-party LLM providers have undergone independent statistical validation for the accuracy of their outputs. These validations are often conducted by external experts or through peer-reviewed research to ensure that the models meet industry standards for accuracy. The results of these validations are generally published in research papers or made available through the provider's documentation.

These responses focus on factual information related to the third-party LLM providers, without making any assumptions about the SaaS company's own practices beyond relying on the third-party provider's assurances.

13

Does Bigtincan send my data to 3rd parties for model training?

Bigtincan does not send customer data to third parties to train their models. When Bigtincan leverages third-party models, we ensure that available privacy and safety settings are configured to limit the disclosure, storage, and use of your data for model training purposes.

14

Do I have a choice in what LLMs I can use?

Bigtincan's AI features can integrate with customer cloud infrastructure (as determined at discovery). For third-party managed models, including GPT models, we leverage managed cloud infrastructure like Microsoft Azure, Amazon Bedrock, and the like.

15

Will my data be used to create, develop, or improve AI features in the product?

No. However, users feedback provide on the accuracy or effectiveness of an AI-based feature sets may be used to improve our AI offerings and/or to inform future product development.

16

Will product users know when or if they are utilizing an AI-based feature?

Yes, we prioritize transparency and the choice of AI in our featureset. Our AI Iconography or phrases like "powered by Genie" indicates our generative AI features in the interface, so users are informed when they engage with generative AI technology.

17

Does the product provide alternatives or opt-in/out functionality for AI-enabled features?

Bigtincan's generative AI features are opt-in by default.

18

What data privacy standards do Bigtincan generative AI features abide by? How are these standards tested?

Our privacy standards are disclosed on our SecureGLP white paper. Bigtincan generative AI features meet Bigtincan's best-in-class data privacy and security standards, including certification in SoC2, ISO27001, and CStar. Our products are tested and vetted by leading security tools and penetration testing (more from GRC here, maybe).

To learn more about Bigtincan's security and data privacy standards, please visit our platform security page and privacy policy at www.bigtincan.com.

19

How do Bigtincan's generative AI features handle content permissions?

Customer data security is a priority. Our AI features always respect established content permissions and access controls. GenieAI only processes content that a user has permission to access, ensuring that responses are based solely on content available to the user.