yabble

Trust your data is secure with Yabble.

At Yabble, we prioritize security to protect your valuable data. Our comprehensive and multi-layered security measures have been meticulously implemented to provide a robust and secure environment for your information.

How is Yabble able to wall off our proprietary data from OpenAI?

Yabble is a Walled Garden. Walled Gardens are protocols ensuring your data is protected and remains confidential at all times.

Yabble is a wholly separate company to OpenAI. Yabble has an enterprise agreement with OpenAI, and has negotiated to ensure that any data run through the Yabble platform is done via API to OpenAI. OpenAI does not use data submitted by customers via our API to train OpenAI models or improve OpenAI's service offering.

The data that is imported into Yabble is stored with Yabble not OpenAI and does not become public. So, when you use Yabble, you are getting all of the benefits of OpenAI's Large Language Models in a fully secured environment.

Where are your servers located?

The Yabble service is hosted within AWS Sydney.

Is Yabble SOC2 compliant?

We adhere to the SOC 2 framework, ensuring our security practices meet and exceed the high standards established by the American Institute of Certified Public Accountants (AICPA). This approach demonstrates our commitment to maintaining a strong and consistent security posture.

Is Yabble GDPR & CCPA compliant?

Yabble is both GDPR & CCPA compliant. Refer to our Privacy Policy for more information.

What dataset is the foundation for the Yabble algorithm?

Yabble uses a combination of our own custom-built algorithms and OpenAI's world-class GPT-3, 3.5, & GPT-4 neural network.

How does Yabble store and transfer data?

We employ cutting-edge encryption standards for both data at rest and data in transit to ensure maximum security for your information. Our data retention and deletion policies comply with industry standards.

Is the data used to train models just for me or do all users benefit from it?

Because Yabble operates a walled garden approach, your data is only training the models in your organization's Yabble environment. Our multi-tenant environment is designed with strict access controls and logical partitioning, safeguarding each client's data while maintaining the highest levels of performance and reliability.

What are the security limitations of the Yabble AI model?

Yabble's AI technology will not scrub your imported data for personal information. We encourage and request any data that is uploaded into Yabble to be de-identified, thereby minimizing risks associated with handling personally identifiable information (PII) and maintaining data privacy.

Our unwavering commitment is to ensure the safety, integrity, and confidentiality of your data. Should you have any questions or concerns regarding our security measures or wish to discuss any aspect in more detail, please do not hesitate to contact us.

For answers to this, that, and everything. Yabble it.

Talk to the Yabble team today at **www.yabble.com**