AutogenAI's Technical FAQ

Do you use open source LLMs?
Not by default. Our approach is to select the most effective LLM for the specific task at hand. Presently, closed-weight LLMs perform better than open-weight LLMs in almost every scenario, hence our preference for closed-weight LLMs. Our team of researchers continuously evaluates the performance of new releases and may consider transitioning to an open-weight LLM if it proves to be more effective in meeting client needs, but only with client consent.
We are happy to discuss custom LLM requirements as part of bespoke solutions, including deployment and use of open-weight LLMs.

(Note: in the context of LLMs, we talk about open and closed 'weights' rather than 'source')

Do they use our data to train their models?
No. Your privacy and data are paramount to us. We never train models on your data, and neither do any LLM providers that we use. This is assured through contractually binding Zero Data Retention agreements which we have reached with each provider, and which prevent them from retaining or learning from your content in any way.

What specific models and providers are you using?
We normally agree the choice and location of LLMs and LLM providers as part of onboarding, and will always notify and receive approval for any changes in choice of provider during contract delivery.

We may use the following providers:

OpenAI (GPT-3.5, GPT-4)
OpenAI servers are located in the USA. They are SOC 2 compliant, undergo annual penetration testing, and comply with GDPR and CCPA. OpenAI do not retain, train on or learn from our data.

Azure (GPT-3.5, GPT-4 by OpenAI)
Azure OpenAI servers are available in many regions including the USA, EU, UK, and Australia. Azure OpenAI services are FedRAMP authorised. Microsoft and Microsoft Azure possess numerous security accreditations including SOC 2 and ISO 27001. Azure OpenAI does not retain, train on or learn from our data.

AWS (Command by Cohere, Claude 2 and Claude 3 by Anthropic, Large and Mixtral by Mistral)
AWS offers Bedrock and SageMaker LLM services. These services host models created by numerous LLM developers. Both services are governed by standard terms, and we have confirmed that neither service retains, trains on or learns from our data. They also do not give any third-party LLM developers access to our data.

Cohere (Command)
Cohere servers are located in the USA. Cohere are SOC 2 compliant and undergo annual penetration testing. Cohere do not retain, train on or learn from our data.

Google (Gemini)
Google Gemini servers are located in the USA. Google Cloud Platform possesses numerous security accreditations including SOC 2 and ISO 27001. Google Gemini does not train on or learn from our data.

Anthropic (Claude 2, Claude 3)
Anthropic servers are located in the USA. Anthropic are SOC 2 compliant, undergo annual penetration testing, and comply with HIPAA. Anthropic does not train on or learn from our data.

Can we plug our models into your engine?
Not by default. However, this can be discussed as it may be possible via custom deployment.

Where is my data stored?
Client data is stored in secure AWS data centres in the client's preferred region. For example, within the UK, USA, Australia, Canada etc.
AWS services are provided under a standard agreement. AWS possess numerous security accreditations including ISO27001, SOC 2, and (for most services) FedRAMP authorisation through JAB. We can host in any AWS region by agreement, including GovCloud.

How is my data protected?
We store your data on hardened infrastructure in secure data centres in the geography of your choice. Your data is encrypted at rest and in transit, and it cannot be accessed by anyone without proper authorisation.

The only places outside of these data centres that will ever see your data are logged-in, authorised users. These are LLM providers with whom we have Zero Data Retention agreements. This means that your data is not retained, inspected, or trained on. When using our application's internet search facility, we connect you with an internet search provider that matches your query to webpages with relevant content.

Why should we trust you?
We meet all the major international information security standards including ISO 27001, ISO27017, ISO27018, CSA STAR, and SOC 2, with regular audits by Schellman and BSI Group. We follow the NIST CSF and NCSC CSG standards for cloud security. We adhere to GDPR and CCPA requirements and undergo regular independent data privacy audits. We commission third-party penetration testing regularly, with additional assessments after major architecture changes. Our online services are under constant, active security monitoring, supported by 24/7/365 in-person response to any alerts. Our dedication to security has earned the trust of some of the most security-conscious organisations in the world, making us an ideal partner in meeting your security needs.