A white paper with black writing

Description automatically generated

The AI powered chatbot will be used to increase efficiency of the customer service side of the company. It will decrease waiting times for customers, and relief the human representatives of more work. However, for it to be effective to its goal and prove useful to the users, it must be built accurately. When I say accurately, I mean the goals must be constantly reviewed and up to date, so the model that is created for the AI chatbot is built upon the correct data that is relevant. Aswell as creating an accurate product, it must also abide by the many strict standards of laws in the UK when it comes to handling sensitive information (such as the Data Protection Act 2018 or the General Data Protection Regulation). This is especially essential due to the potential sensitive information that customers may omit to the AI chatbot, and any guidance or advice the AI may provide must be meticulous.

I have chosen the widely popular ‘CRISP-DM’ (Cross-Industry Standard Process for Data Mining) methodology. This is due to it being data driven and is aligned with the business’s needs.

The original CRISP method does not contain Continuous Delivery and Integration (CD/CI), since this is found in more DevOps methodologies. However, it is possible to integrate CD/CI practices to include robust and efficient deployment of versions of the AI chatbot. This can be done be enhancing the phases (not adding new ones) with automation, live feedback/ monitoring and pipelines. For example, when creating the model in the ‘modelling’ phase, it will be automatically trained with the dataset. This will dramatically improve the production time and response to improvement suggestions.

Though security Integration is not explicitly addressed in the standard framework. It can be easily established in the existing phases. It will largely consist of securing the data that is being collected and used to test models. This will be achieved through encrypting the data, and rigorously testing attacks on the system (such as penetration testing or simulating a Denial-of-service attack).

Overall, this lifecycle with a few easy implementations would be an incredibly effective method on developing an AI chatbot.