BHBIA
ETHICS & COMPLIANCE

Use of AI in Market Research

June 2024

Definition of AI

There are numerous definitions of Artificial Intelligence (AI) that are widely used, this may be because various types of AI have a definition of their own and AI is largely used as an "umbrella term".

ICO refers to AI in 2 different contexts – one definition used by research community and another adopted to use in data privacy context (ref: ICO Guidance on AI https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/about-this-guidance/)

- In the AI research community, it refers to various methods 'for using a non-human system to learn from experience and imitate human intelligent behaviour'; or
- in the data protection context, 'the theory and development of computer systems able to perform tasks normally requiring human intelligence'.

European Parliament, currently working on AI regulatory framework, defines AI as the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity.

Regardless of definition, the emergence and fast adoption of Large Language Models and Generative AI (e.g. ChatGPT), as well as their potential to significantly increase productivity and efficiency of services has led to significant concerns about its safety, impact on individuals and data privacy, accuracy, bias and potential for discrimination.

Types of AI already used in Market Research and Data Analytics

- **Predictive Analytics:** AI models can analyse historical data to make predictions about future trends, enabling organisations to make decisions.

- **Customer Segmentation and Personalisation:** AI can analyse customer behaviour and preferences to segment them into distinct groups, allowing for targeted marketing and personalised recommendations.

- **Consumer Insights from Unstructured Data:** AI-powered Natural Language Processing (NLP) can extract insights from unstructured data sources like customer reviews, forums, and social media.

- **Image and Video Analysis:** AI can analyse images and videos to identify objects, patterns, and even emotions, which is valuable in industries like healthcare, retail, and security.

- **Sentiment Analysis:** AI can determine the sentiment expressed in text data, allowing organisations to understand public opinion about their products or services.

- **Ad Campaign Effectiveness:** AI can analyse the performance of advertising campaigns by tracking metrics like click-through rates, conversion rates, and return on ad spend.

- **Competitor Analysis:** AI can scan and analyse vast amounts of data about competitors, including product features, pricing strategies, and customer reviews.

Considerations for processing of personal data when using AI

Below are the aspects that should be considered when processing personal data using AI models or applications:

- Transparency – how personal data is being processed within AI system, including purpose for processing, data retention periods, and who the data will be shared with. Important to note that LLMs (such as ChatGPT) store information that is provided to them and "learn" from it, in order to improve on their answers next time. It is, therefore, paramount that no sensitive or confidential data is uploaded to them (particularly free/unlocked versions).

- Lawful basis – have appropriate lawful basis for processing of personal data. Lawful basis has to be determined prior to processing; decision making should be documented. Lawful basis needs to be included in privacy notice. Consent is considered appropriate lawful basis when there is a relationship with the data subject, but consent will need to be freely given, specific, informed and unambiguous, and involves a clear affirmative act on the part of the individuals.

- Accuracy – this term has different interpretations depending on whether it is accuracy within data protection or accuracy of AI. Accuracy of data under data protection is one of the fundamental principles, requiring organisations to ensure that personal data is accurate and not misleading. Accuracy within AI is frequency of AI system to "guess" the right answer. Whilst accuracy in data protection applies that data must be 100% accurate, AI systems might not be 100% accurate and would represent "statistically informed guess".

- Fairness – In AI, fairness means that processing will have no detrimental effect on individuals and avoids discrimination.

- Safety and security – ensuring appropriate levels of security when processing personal data, to protect against unlawful and unauthorised access, accidental loss, destruction and damage.

BHBIA
ETHICS & COMPLIANCE

Other considerations

- Bias and discrimination – AI systems may learn from historical data that might be unbalanced and therefore produce discriminatory decisions.

- Locked vs unlocked AI solutions: unlocked AI solutions may be based on larger data sets but are likely to be less secure. “Locked” AI solutions may be more secure but will be limited in what they have been trained on and be less accurate. Locked AI solutions are usually those that are limited to an organisation and are not open to public use (e.g. an internally created AI application that is created using test data but is limited to the use within the organisation only and the data is not shared externally). “Unlocked” AI solutions are public and any information input into them can be used to further train the public model (i.e. not confidential).

- Where machine learning is used to generate analysis, it is not always possible to determine how the analysis has been conducted, and the method may also change from time to time. This may need to be considered if outputs require compliance approval.

Upcoming legislation - EU

EU Council has approved the long-awaited EU AI act on the 21st of May 2024, completing its legislative process. Whilst the text will not be available for a number of weeks, once published in the Official Journal of the EU, it will come into force 20 days after publication and will be fully applicable 24 months after coming into force (mid-2026).

The EU AI Act is in stark contrast to the UK’s white paper on AI, and focuses on placing legislative obligations on AI developers, classifying AI tools in systems in 4 distinct categories, placing bans on “Prohibited AI practices” that includes facial recognition technology in public places, social scoring AI and Emotion-recognition AI. It will also place significant fines on any breaches to “Prohibited AI practices” to the tune of € 30.000.000 or 6% of global turnover for offending companies and will be regulated by a newly established network of regulators. This is different to the UK where instead of giving responsibility for AI governance to a new single regulator, the government will empower existing regulators - such as the Health and Safety Executive, Equality and Human Rights Commission and Competition and Markets Authority - to come up with tailored, context-specific approaches that suit the way AI is actually being used in their sectors.

This contrast between the UK and EU approach to AI is likely to leave significant gaps between UK and EU legislation, creating practical challenges for companies developing and using AI that are likely to be used in both the UK and the EU.

Further reading: https://www.lexology.com/library/detail.aspx?g=2f340a18-81d7-4aa9-b883-d473d9170fa4

The US approach to AI regulation

The “US Blueprint for AI bill of rights” whilst not an enforceable legislation, it is a guide to society that protects the American Public in the age of Artificial Intelligence. It outlines 5 key principles by which AI models need to be designed and deployed. These are: safe and effective systems, algorithmic discrimination protection, data privacy, notice and explanation, human alternatives, consideration and fallback.

Similarly to the UK, there are significant differences to this approach vs that in the EU. Whilst both share vision to risk-based approach to AI, there are significant differences of opinion, particularly when it comes to socio-economic processes and online platforms and more will need to be done to ensure alignment in dealing with emerging AI technologies.

References and useful links:

The ICO Guidance on AI and Data protection
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

MRS Guidance on using AI and related technologies DRAFT.
https://www.mrs.org.uk/standards/guidance-on-using-ai-and-related-technologies

Government’s “Pro-innovation approach to AI regulation” white paper
https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#:~:text=The%20white%20paper%20sets%20out,approaches%20to%20governing%20AI%20develop.

EU AI Act
https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Blueprint for an AI Bill of Rights
https://www.whitehouse.gov/ostp/ai-bill-of-rights/

Produced by the BHBIA’s Ethics & Compliance Committee June 2024

British Healthcare Business Intelligence Association
St James House, Vicar Lane, Sheffield, S1 2EX
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455