# Artificial Intelligence (AI)

• Find out what Responsible AI is?

• Find instances where AI has failed? Or been used maliciously or incorrectly.

• Implications of when AI fails. There is a specific article in the GDPR Law that covers this, especially with automated decision making. (opt in and out options).

• What should organisations do to ensure that they are being responsible with AI and the wider use of data in general?

• Maximum 500 words.

Responsible AI is a best practice framework to ensure implementation of AI is responsible and governed. It is a set of practices used against datasets to ensure the outputs are legal, explainable and have reduced bias.

An example of where AI has failed are due to failings of best practice. Such as Microsoft Tay (bot), which was originally designed to mimic language features. However, once it was made live through Twitter, it mimicked the language of a small group of internet “trolls”, so resulted in sexist and racists tweets and was taken down 16 hours later. You can argue that this is a result of poor validation testing and not considering all possible outcomes.

GDPR Article 15 allows the data subject to have access to any automated decision-making process or logic involved. Meaning any AI systems that process personal data will need to ensure that any information involved is properly controlled and the data is appropriately trained. GDPR Article 22 extends on Article 15, allowing the data subject the right to not be profiled and offer an explanation around the parameters of the algorithm. Obviously, if AI fails under GDPR law sizeable fines are likely to be imposed on the company, examples of this are H&M receiving a 32million euro fine for profiling employee’s following sickness absences which was then used in performance reviews.

AI presents complications with GDPR, as some AI systems may hold onto data far longer than they need to for future machine learning (ML). However, this could be combated by using ML to trawl through any data collected and remove the identifiable information and data which has been kept for longer than needed.

In order for originations to be more responsible with data, it needs to be legal collection of data and opt-in and opt-out mechanisms need to be easily accessible, to prevent data collection by ease such as unscrupulous opt-out cookie requests. GDPR law application has started to combat this by imposing fines on Amazon and Google, to ensure appropriate collection mechanisms for data used within AI.