ARTIFICIAL INTELLIGENCE (AI)

1. Find out what Responsible AI is?

Responsible AI is a governance framework that documents how a specific organization is addressing the

Challenges around artificial intelligence (AI) from both an ethical and legal point of view. As practice Responsible AI is the practice of designing, developing, and deploying AI with good intention to empower employees and businesses and fairly impact customers and society – allowing companies to engender trust and scale AI with confidence.

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

* Microsoft’s AI Chatbot Tay – targeting its vulnerabilities trolls on microblogging website manipulated Tay into making deeply sexist and racist statements.
* Amazon’s AI-Powered Recruiting Tool - its Machine Learning specialists build the programme that had taught their own AI to prefer male candidates over female ones.
* Google Photos AI Panorama – Google Photos uses AI throw up enhanced versions of photos taken by users on their smartphones, however a relatively obscure features can automatically detect images with the same backgrounds and merge these into a single picture.
* Facial Recognition Failure in Chine – Traffic police in major Chinese cities deploy smart cameras that use facial recognition techniques to detect jaywalkers, whose names and faces then show up on a public. They wrongly shamed a billionaire businesswoman after a facial recognition system deigned to catch jaywalkers caught her on an advert on a passing bus. CloudWalk researcher explained that the algorithms lack of live detection might been the problem.
* Amazon’s facial recognition – Members of US Congress rained down on Amazon after its facial recognition falsely matched 28 congress people with mugshots of criminals. According to the American Civil Liberties Union (ACLU) nearly 40% of the matches were of people of colour indicating that the technology is racially biased.

1. 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).

The UK GDPR gives people the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them. These provisions restrict when you can carry out this type of processing and give individuals specific rights in those cases.

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

Under GDPR when you collect personal data you have to say what it will be used for and not use it for anything else. You cannot collect data simply to do a ML trawl on it. Specific uses of AI may be more acceptable such as using data to calculate a credit score but even then, you must take care that the scope of the credit scoring system does not widen. Always try to minimise the data you hold.