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. An important goal of responsible AI is to reduce the risk that a minor change in an input's weight will drastically change the output of a machine learning model.

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

1.Face ID Hacked Using a 3D Printed Mask

Facial recognition is cropping up everywhere nowadays, but it may not be as secure as we initially thought. Researchers have been able to find instances in which facial recognition has been fooled using a 3D-printed mask that depicts the face of the face used to authenticate the Facial ID system.

2. Robot passport checker rejects Asian man's application because "eyes are closed."

After attempting to renew his passport, Richard Lee, a 22-year-old man of Asian descent, was turned down by the New Zealand Department of Internal Affairs after its software claimed his eyes were closed in his picture.

The facial recognition software rejected Lee's photo, and Lee had to contact the department in order to speak to a human and get his new passport validated.

AI Automated Decision making and the GDPR:

Algorithms are used as a tool for automated decision making, including profiling, to discover individual preferences, predict behaviours, and/or make decisions that may impact individual's rights and interests. The General Data Protection Regulation (GDPR) has put the control over how personal data is used firmly back with the individual.

Article 22 of the GDPR states that individuals have the right not to be subject to a decision that has a legal or similar effect upon them and, that is based solely on automated decision-making (without human intervention). There are some exemptions to this right; where the use of personal data is necessary to enter into a contract, if the processing is authorised by law or if explicit consent is given by the data subject.

However, even when applying exemptions, organisations must still ensure they are protecting (and be able to demonstrate how) the rights, freedoms and interests of individuals. At the very least, they must ensure the right to human intervention if requested and, in doing so, ensure that individuals have not been disadvantaged through this process.

To ensure that any processing of personal data is lawful, fair and transparent, individuals should be provided with specific, clear and meaningful information about how automated decisions are being made about them.

To avoid the ‘computer says no’ effect and, to meet their data protection requirements, organisations need to plan the implementation of new AI technologies carefully with a specific focus on protecting individual rights.