**Responsible Artificial Intelligence (AI)**

Responsible AI is a framework set up to specify how organisations handle the problems that arise around their use of artificial intelligence from both the moral and lawful perspective. This framework tries to sort out situations where wrongdoing has been identified in the use of artificial intelligence by an organisation and the organisation needs to take action to rectify the situation and handle the aftermath.

However, the framework has not been specifically laid out for all data analysts ranging from software developers to data scientist, the framework to prevent unethical and illegal artificial intelligence usage vary among different organisations. Many people are still hoping for a largely accepted framework to verify the right AI practices to make sure that AI programming equally considers various factors and is easily understandable.

**FAILED AI EXAMPLE**

When Apple released the iPhone X , they replaced the fingerprint lock detail with the facial recognition as the basic passcode. The facial recognition feature made use of the iPhone front camera and machine learning to create a 3D map of the user’s face. The machine learning/AI component helps the phone system to adjust to changes from the user like use of makeup, wearing glasses or a scarf on the neck. All these were said not to affect security of the device.

However, few days after the iPhone X launch, hackers were able to bypass the face recognition passcode using a 3D printed mask. Bhav a security company located in Vietnam realised they could unlock the iPhone X face ID feature by putting 2D eyes on a 3D mask. The mask was made from stone powder and were priced at £200 while the eyes were easily printed infrared images.

This finding gained attention worldwide as Apple has originally said that face ID was designed to safeguard against the same use of masks by hackers using advanced neural networks. However, not everyone believed Bhavs finding as other companies had tried and failed, but this showed that Apple new technology using AI had some interesting weaknesses.

**Implications of when AI fails - GDPR Law (opt in and out options).**

AI is not specifically mentioned in GDPR, however, many of the GDPR practices are useful in AI practices. Issues concerning data protection principles are addressed in GDPR especially when the purpose of the AI programme fails and doesn’t meet all ethical and legal requirements.

Data protection principles:

* Purpose limitation: The collection of data should be limited to the purpose it was collected for. Limits reusage of data.
* Data minimisation: Reduce the ease with which data can be linked back to the individuals.
* Special treatment of sensitive data.

**Organisations AI processes.**

The GDPR principles should be considered by organisations when carrying out AI -type processes while considering the complex nature of AI application. Subjects’ data used in the AI process should be made to understand the purpose and methods their data will be used and possibly the possible setbacks.