Home Learning Task 8

Compulsory HLT:

Practical: Artificial Intelligence (AI)

In Data Science we process a lot data through AI. With the GDPR, it is becoming increasingly important to understand the ethics behind the data that is collected, stored, processed and evaluated.

Your task is to:

Answer to HLT 8, Compulsory HLT	
• Find out what Responsible AI is?	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 create trust and scale AI with confidence.
• Find instances where AI has failed? Or been used maliciously or incorrectly.	• Privacy violations. • IBM Watson health care • Tesla cars crash due to autopilot feature. • Amazon's AI recruiting tool showed bias against women. • Microsoft's AI chatbot turns sexist, racist.
• 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).	Implications of when AI fails can include privacy violations due to personal data breaches. Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
• What should organisations do to ensure that they are being responsible with AI and the wider use of data in general?	Using model of best practice and checklist • Cary out Data Protection Impact Assessments (DPIAs) to consider and address the risks before starting any new automated decision-making or profiling. • Tell customers about the profiling and automated decision-making carried out, what information used to create the profiles and where to get this information from. • Use anonymised data in profiling activities. • Have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy. • Send individuals a link to our privacy statement when obtaining their personal data indirectly. • Explain how people can access details of the information used to create their profile. • Tell people who provide with their personal data how they can object to profiling, including profiling for marketing purposes. • Have procedures for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues.

	• Have additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children). • Only collect the minimum amount of data needed and have a clear retention policy for the profiles created.