# Responsible AI

Artificial intelligence is the use of computer programming to mimic human intelligence, this has benefits across a range of fields especially in the realm of big data where businesses and numerous enterprises are trying to make sense of large quantities of data. With all the great things brought about by AI, automation of human tasks has its limitations and downsides.

Responsible AI aims to stress the importance of accountability and transparency from both an ethical and legal point of view. General Data Protection GDPR is an EU law on the regulation of data protection and privacy. It sets out to impose rules and guidelines on the data collection and processing of individuals’ personal information in the EU. The need for regulation is a result of the increasing threat from individuals with malicious intent such as hackers, fraudsters etc and other groups of individuals with sinister motives. When AI fails or becomes compromised the impact can have far reaching consequences. One such example is when the AI used in facial recognition technology by Apple failed, hackers were able to bypass the security feature using a 3D printed mask. The AI was unable to differentiate a human face from that of a 3D printed version sparking privacy concerns.

The GDPR directive places responsibility for compliance on any business or data gathering entity operating in the EU to safeguard and use collected data responsibly. It provides these entities with guidelines and tools to demonstrate compliance and legal action is an option if any of the directives in the regulation are not abided by. The seven principles of the GDPR are as follows:

**Lawfulness, fairness, and transparency**

This means having legitimate grounds for collecting data and not using it in any way that may have unjustified adverse effects on the individual. An organisation must obtain the data in a manner that is not coercive or under false pretence. Individuals also have the right to be informed about how their information is to be used.

**Purpose limitation**

Information about individuals collected by businesses and other entities should only be obtained for specified purposes and used as such.

**Data minimisation**

This principle states that data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy.

**Accuracy**

This refers to how information is processed, stored, and updated. It is a requirement that personal data is kept up to date and if inaccurate, that data is rectified and updated without delay.

**Storage limitation** Organizations should perform periodic reviews to identify, and address, data stored beyond intended use. So, even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you need it.

**Integrity and confidentiality (security)**

Confidentiality means that data, objects, and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct.

**Accountability**

The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.