Responsible AI is a *governance framework* that documents how a specific organisation is addressing the challenges around Artificial intelligence (AI) from both an ethical and legal point of view.  Resolving ambiguity for where responsibility lies if something goes wrong is an important driver for responsible AI initiatives.

Responsible AI (RAI) is the only way to mitigate AI risks.  Now is the time for developers/organisations to evaluate their existing practices or create new ones to responsibly and ethically build technology and use data, and be prepared for future regulation.  Future payoffs will give early adopters an edge that competitors may never be able to overtake.

Instances where AI has failed or been used maliciously or incorrectly - AI has made a monumental contribution to humanity and since it's just another tool in technology, its failures have also been huge. In this article, the AI could not match the photo presented by an applicant for a passport, indicating that the applicant closed his eyes - AI was considered as being racist!  Another instance in this article was that AI was not able to crack an entrance examination.  AI on this occasion was not able to understand the question that requires the ability to grasp the meaning in a broad spectrum.  Thirdly, Amazon's smart assistant Alexa created a problem for the owner who was absent from home that warranted the neighbours to call the police who broke into the property to turn off the music that was playing loudly.

Malicious use of Artificial Intelligence refers to the use of AI and machine learning to augment offensive cyber-attacks, enabling adversaries to launch highly targeted and sophisticated attack campaigns at greater speed and scale than ever before.  AI has been used to threaten digital security (for example, through criminals training machines to hack or socially engineer victims at human or superhuman levels of performance), physical security (e.g. non-state actors weaponising consumer drones), and political security.

Source: [Top 5 Epic Artificial Intelligence Fails (analyticsindiamag.com)](https://analyticsindiamag.com/top-5-epic-artificial-intelligence-fails/)

AI fails when there are incorrect predictions which can cause enormous harm if left unaddressed and unaccounted for.  The likelihood of AI system failures makes *AI high-risk in and of itself* - and especially if not monitored correctly.

Implications:

* If AI fails to recognize and match images, there is a problem
* AI can despise humans
* AI development to fight cancer could kill patients if it fails
* AI for secure system access by a face can be tricked with a mask and thereby fails to recognise the right person and possibly, grant access to the wrong person.

Organisations are always at the receiving end of AI success or otherwise.  Organisations should take full responsibility to ensure compliance with the relevant provisions of the GDPR, particularly, Article 22 which covers "automated individual decision-making, including profiling."  Even though some see Article 22 as prohibitive to some extent, it is generally believed that GDPR could also "help create the trust that is necessary for AI acceptance by consumers and governments."