WK 6 Artificial Intelligence (AI)

What is Responsible AI

Responsible AI is a framework for bringing many of these critical. practices together. It focuses on ensuring the ethical, transparent and accountable use of **AI** technologies in a manner consistent with user expectations, organizational values and societal/Government laws and norms. (ref Google)

There are about 6 common known AI failure reported online involving big companies like IBM, Microsoft, Amazon etc. Four examples are listed below:

Microsoft’s AI Chatbot Corrupted by Twitter Trolls

Apple’s Face ID Defeated by a 3D Mask

Amazon Axes their AI for Recruitment Because Their Engineers Trained It to be Misogynistic

Amazon’s Facial Recognition Software Matches 28 U.S. Congress people with Criminal Mugshots

(Reference Google)

Implications when AI fails (GDPR)

The General Data Protection Regulation (GDPR). GDPR extensively regulates AI, in relation to autonmous decision making the customer is given the option of opting in or out for example

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.

Finally, there are provisions of the GDPR that specifically address some of the common issues and risks associated with AI, such as those relating to the data protection principle of data minimisation and the requirement that personal data be processed lawfully and fairly.

When AI fails then sanctions and fines apply, every organisation has to have measures and policies in place to ensure AI runs fine however if it fails or there is breach in data then the ICO (Information Commison Office) has to be notified straight away and advised what measures have been taken.

What should organisations do to ensure that they are being responsible with AI and the wider use of data in general?

Organisations should have internal governance or a review panel to check the adherence to regulations/procedures and have knowledge of the implications of possible failures of AI.

They should ensure the right technical guardrails are in place, creating quality assurance and governance to create traceability and auditability for AI systems.

This is an important part of every organisation’s toolkit to allow operational and responsible AI to scale.

They should Invest more in their own AI education and training so that all stakeholders – both internal and external – are informed of AI capabilities as well as the pitfalls.

The GDPR is underpinned by a number of data protection principles that drive compliance. These principles outline the obligations that organisations must adhere to when they collect, process and store an individual’s personal data.

The key principles are: Lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability.

While the data protection principles are similar to those found in the previous Data Protection Directive (DPD), they are more detailed to ensure greater levels of compliance and to take into account advancements in technology.

With regards to wider use of data in general I believe organisations have to follow the 7 principles of GDPR, but compliance is key otherwise an organisation can be fined 4% of their annual turnover.

Reference (What are the principles of GDPR, Geraldine Strawbridge, July 1st 2019)( 3 ways organisations can use AI, Kate Rosenshine, 08/01/2020).

Extension- Investigate the 3 challenges in AI (Talent, Time and Trust)

Talent is the first challenge. Organisations need to hire, train, assemble and partner with the right expertise. A team of talented individuals that are capable of driving the AI transformation needs to be created and utilised fully.

Data experts are needed to build models and algorithms, they also require people with different technical abilities that allow them to uncover useful insights from the data, before passing it on to the experts. Doing this can help train the existing workforce, since they have the essential domain experience for the job. ML (Machine Learning) is as much of a cultural transformation as it is a business one. Instead of rebuilding an entire team from scratch, companies should look to hire several data scientists and utilise the existing pool of experienced staff to assist them.

Time is needed to deliver AI strategy and this can involve determining outcomes: Asking the right questions determines what outcomes can be generated from any specific application. The main idea here is to translate the high-level goal of your company into a business problem, and subsequently determine the outcome.

Measuring Success: Companies must also identify metrics that can measure its success. The definition of success may vary for different companies, but the end goal remains the same; making a profit and delivering value.

Connect With the Community: Community plays a vital role in driving change in any company. There are many ways to connect with the machine learning community, including online and webinars, as well as offline at meetups, when the time is right again for that. These will enable community members to exchange knowledge and learn from each other. Learning from each other, participating in sessions and sharing relevant insights are great ways to connect with the community, regardless of where you are.

Trust

Being able to describe the model’s decision adequately, having sound documentation and eliminating bias from the results are key considerations for companies, in order to instil trust in AI. Deciding what technology to use is important, as this can have a profound business impact. For example companies have to decide between open source or proprietary software, or perhaps even both. Cloud or on-premise environments: This depends on how soon you would like to begin. If you are starting from scratch and do not have an existing DevOps system in place, it’s easier to get started on the cloud. This eliminates the need for procuring and setting up software, as well as security, infrastructure and maintenance issues. However, if you do already have a decent DevOps infrastructure in place, the on-premise option can help optimise costs. Many companies also prefer the hybrid model, where they are able to switch between cloud providers and on-prem, which is good practice.

(reference How to effectively deliver an AI transformation strategy, John Spooner 15th April 2020) Google.