DATA GOVERNANCE AND MANAGEMENT

Chijioke Franklin Emejuru

Project Description: This project examines data governance, GDPR compliance, ethical AI issues, and cloud computing sustainability.

Project Overview: The project provides a detailed analysis of various aspects of modern data management, including the roles of information officers, data custodians, and the Chief Data Officer in data governance. It also highlights key data protection regulations under GDPR, focusing on consent, data subject rights, and the secure transfer of data. Additionally, the project examines ethical challenges in AI, such as accountability, bias, and explainability, offering potential solutions for these issues. Finally, it explores the sustainability benefits and challenges of cloud computing, emphasizing energy efficiency, resource optimization, and the importance of responsible e-waste management.

1. In a Data Governance Operating Model, roles and duties at the operational level often include:

Operational Level: Information officers: They are officers in charge for monitoring data quality and ensuring data accuracy in operating systems. In the retail sector, for example, an information officer may be responsible for ensuring the accuracy and integrity of product information inside the inventory management system. As a data steward, they regularly monitor data quality, resolve discrepancies, and work with store employees to enhance data entry processes. This guarantees that inventory data is trustworthy, allowing for seamless operations and customer assistance.

Tactical Level:
The Chief Data Officer (CDO) is responsible for developing and communicating the organization's data governance structure. It is their responsibility to ensure that these governance standards are consistent with the company's strategic business goals. For example, in a financial organisation, the CDO may develop a data governance policy that prioritises data security measures and uses sophisticated analytics to identify fraud. Their emphasis would be to link these activities to the overarching goal of safeguarding client assets and maintaining regulatory compliance.

Operational Level:
Data custodians: implement and administer the security measures necessary to protect private information, ensuring that data storage and access requirements are followed. In a hospital, for example, a data protector may oversee safeguarding patient health information to ensure privacy. They guarantee that only authorised users have access to the proper data from storage systems and that all regulatory criteria are met to protect patient privacy and data security.

Tactical level:
Data governance: It is the process of creating and evaluating standards and methods that help schools manage their data well, deal with important governance issues, and make smart choices. In a university setting, the data governance board can set clear rules for keeping an eye on student data so that all academic areas follow the same rules. The people would set rules for how data should be categorised and used. They would also deal with current issues, like making sure that data privacy rules are followed in educational research. This makes sure that the school is honest and open about how it uses student information, which builds trust and dependability in the educational community.

2. As the Data Protection Officer (DPO), I can offer expertise on the scope and obligations of GDPR and the Data Protection Act in Ireland, as well as address the issue of data transfers to the United States and the UK.

Consent: It is the authorization to handle personal data that is either required by law or obtained directly from the individual whose data is being processed. Many individuals are aware that consent is one of the six legal bases for processing personal data under the General Data Protection Regulation (GDPR). However, it is vital to note that consent is not the sole reason. Article 6 of the GDPR includes additional reasons, including contractual obligations, legal requirements, the data subject's vital interests, public interest, and legitimate interests [1].

Data protection and regulation (right of individual): The goal of the General Data Protection Regulation (GDPR) is to provide people more power and control over the data that belongs to them. The GDPR's section on data subject rights, which covers each right in detail, emphasises this goal. You are entitled to see your data, change it, remove it, stop processing it, move it, object to processing, and stop basing choices only on computerised processing [2].

Data Transfer: It is important for global businesses and international cooperation, especially with the European Union (EU), to be able to send sensitive data across countries. But it is very important to ensure people's information is safe, especially when it is sent to "third nations," which are places outside the European Union. Chapter V of the General Data Protection Regulation (GDPR) has strict rules that make sure this doesn't happen. These rules say that sending personal data outside of the EU/EEA is illegal unless strong security procedures are used to protect it, like standard contracts or accepted processes. For example, if an Irish company plans to transfer customer data to a cloud service provider located outside the European Economic Area (EEA), they must confirm that the provider adheres to the standards of the General Data Protection Regulation (GDPR) [3]. The General Data Protection Regulation (GDPR) says that companies must tell the right authority about any data breaches as soon as they know about them, preferably within 72 hours. Any data leaks that could put people's rights and freedoms at risk must be quickly discussed with the people who are affected by the breach. All data leaks must be recorded and documented by organisations. This includes gathering information about the breach, its effects, and the steps taken to address and fix the problem. For example, an educational institute in Ireland discovers unlawful access to student’s records. By GDPR Article 33, the provider promptly reports the breach to the Irish Data Protection Commission (DPC) and provides all necessary information, including the nature of the breach and efforts taken to mitigate its impact [4].

3. There are three main ethical problems with the use of artificial intelligence (AI):

Accountability: As AI develops more extensively across industries, we increasingly rely on AI technology for everyday decision-making. However, when these behaviours have bad repercussions, it becomes difficult to assign responsibility. Should companies that utilise AI be held liable for assessing the algorithms of the tools they acquire? Should AI tool creators be held accountable? This pursuit of accountability is a hard and intricate undertaking, making it difficult to ensure that individuals and corporations are held responsible for the repercussions of AI-impacted acts. Clarifying responsibilities in the realm of AI is crucial for increasing trust, ensuring ethical use, and mitigating hazards. To hold stakeholders accountable for the consequences of AI-driven operations, well-defined standards, regulatory frameworks, and monitoring methods are required [5].

Solutions: Implement Privacy by Design: Build privacy protections into AI systems from the start, ensuring that data is hidden, encrypted, and only available to those who need to know.

Bias

Another ethical problem is related to AI prejudice. Although AI is not inherently biased, systems are educated utilising data from human sources and deep learning, which may lead to the spread of prejudices via technology. An AI recruiting tool, for example, may ignore certain demographics if the data sets used to train the system are biased against a certain group. This might also have legal ramifications if it results in discriminatory actions [5]

Solution: Make sure the training data is inclusive and appropriately represents the demographics of the individuals it will interact with.

Explainability: refers to the ability to provide a clear and understandable explanation or justification for a particular concept, process, or decision. Mere deployment of AI technologies without active monitoring and supervision is insufficient. Gaining a comprehensive understanding of the decision-making process is especially crucial when dealing with specific AI applications. Understanding the rationale behind the findings reached by various AI technologies might be challenging in certain instances. These consequences may be significant, particularly in areas such as healthcare or law enforcement, where it is crucial to examine influencing circumstances and when the lives of actual people are at risk [5].

Solution: Protect private data while it's being sent and while it's being stored by using strong encryption methods.

4. Cloud computing has various sustainability benefits, including:

Energy Efficiency: Advantage Cloud companies may employ economies of scale to optimise energy use in their data centres, resulting in overall energy efficiency benefits over on-premises equipment.

Cloud companies invest in energy-efficient technology, cooling systems, and data centre design to reduce energy use. Google's data centres utilise innovative cooling technology, such as saltwater cooling, to save electricity [6].

Resource Optimisation: Advantage: Cloud computing enables users to adjust resource levels depending on demand, minimising resource inefficiency.

Cloud services such as Amazon Web Services (AWS) and Microsoft Azure enable organisations to quickly allocate computer resources and adjust capacity in response to demand. This flexibility reduces waste capacity while increasing resource efficiency.

Reduced carbon footprint Cloud computing may help to reduce carbon emissions from traditional IT infrastructure by concentrating computing resources in energy-efficient data centres.

Research undertaken by the Lawrence Berkeley National Laboratory found that cloud computing may result in significant carbon emissions reductions when compared to on-premises data centres. This is mostly due to greater server utilisation rates and increased energy efficiency.

Nonetheless, the use of cloud computing offers significant challenges:

Data Centre Location: Problem: Cloud data centres are grouped in certain places, which could have effects on the environment and make people worry about how to get energy in those places.

For instance, data centres in places where coal is the main source of electricity may release more carbon dioxide than those that get their power from green sources.

E-Trash Management: Problem: Because cloud computing uses a huge network of real parts, it's harder to make and get rid of electronic waste (e-waste) properly.

Given that cloud providers routinely update and decommission equipment, they must utilise appropriate e-waste management procedures to safeguard the environment and prevent resources from running out. When customers transfer data to cloud data centres, network congestion, increased energy consumption, and latency issues might occur.

To overcome these difficulties, cloud providers, governments, and enterprises must work together to adopt sustainable practices such as sourcing renewable energy, establishing e-waste recycling programmes, and implementing efficient data transmission technologies. Although cloud computing has certain limitations, its overall sustainability benefits make it a viable alternative for enterprises aiming to lower their environmental impact while fulfilling their computing requirements.

References:

[1] Consent, ‘*General Data Protection Regulation (GDPR)’*. Accessed: May 9, 2024. [Online]. Available: https://gdpr-info.eu/issues/consent/

[2] Right of individual, ‘Right of access by the data subject| Art. 15 GDPR.’ Accessed: May 9, 2024. [Online]. Available: https://gdpr-info.eu/art-15-gdpr/.

[3] ‘Transfers of Personal Data to Third Countries or International Organisations | Data Protection Commission’, Transfers of Personal Data to Third Countries or International Organisations | Data Protection Commission. ’ Accessed: May 9, 2024. [Online]. Available: https://www.dataprotection.ie/organisations/international-transfers/transfers-personal-datathird-countries-or-international-organisations.

[4] Data Breach, ‘Notification of a personal data breach to the supervisory authority |GDPR Article 33 .’ Accessed: May 9, 2024.[Online]. Available: https://gdpr-info.eu/art-33-gdpr/

[5] Ashley Watters,’ Common Ethical Issues in AI’ Accessed: May 9, 2024. [Online]. Available: https://connect.comptia.org/blog/common-ethical-issues-in-artificial-intelligence

[6] Yenugula, M., Sahoo, S. K., & Goswami, S. S. (2024). ‘Cloud computing for sustainable development: An analysis of environmental, economic, and social benefits. Journal of Future Sustainability, 4(1), 59–66’. https://doi.org/10.5267/j.jfs.2024.1.005.

[7] Zaripov, B., Mirzaliev, S., Sharipov, Z., Xakimov, B., Xudayqulov, R., Aziz, A., & Sharipov, K. (2023). ‘The importance of cloud computing trends and the conceptual model in higher education for sustainable development. E3S Web of Conferences, 401, 03064’. https://doi.org/10.1051/e3sconf/202340103064