We are all aware that the goal of MDM is to consolidate all business-critical information into a single, centralised data source, but it is crucial to implement secure data protection with the required planning and preparation (Sanderson, 2011). Identification of high-risk data by conducting DPIA (data protection impact assessments) and data protection code of conduct to address any data protection issues. Applying data protection certifications in a practical approach helps in data protection (ICO, 2024)

Effective cost-saving measures must be taken into account during planning, which may involve increasing operational effectiveness in addition to IT. The end-to-end data traversing process is well understood, documented, and encrypted as necessary to protect sensitive data from data breaches. Additionally, the businesses have procedures, communications, and transparency in place in case of any cyberattacks (Fortra, 2023).

Before sharing personal information, it is especially important to understand why the information is being shared, who the information is being shared with, and how it will be used. When transferring data to other parties, there must be extra-legal basis for the sharing, restrictions on how long the data may be held, and a mechanism for getting consent. When sharing files, it's crucial to take into account the possibility of unauthorised people accessing your files and transmitting personal information outside of your organisation. In order to address any social or legal issues, companies must get explicit consent before collecting and storing data. Third-party contracts or agreements are maintained to regulate permitted data usage (Shaunessy, 2023). Limitation of liability clauses in the contract should be used to protect the organisations in the event that a liability exposure occurs and data protection regulations are not followed.

Digitisation of MDM will help to implement some of the Data Governance processes. Implementation of Artificial Intelligence powered automation to centralise the business processes and helps in detecting and visualising an attack path. However, it is important to measure the balance between the two kinds of errors, false positive and false negative. The results of the AI system should be statistically accurate enough to ensure that the data processed fairly and lawfully (Barrenechea, 2023).

In summary, there is no one solution to the problem, it requires data scientist to analyse and implement solutions as required to address any data protection issue.

References

Barrenechea, M. (2023) Use cases: ArcSight Intelligence: Micro focus, Use Cases | ArcSight Intelligence | Micro Focus. Available at: https://www.microfocus.com/en-us/use-case/arcsight-intelligence (Accessed: 21 January 2024).

Fortra. (2023) Why Transparency After a Data Breach is Important, terranovasecurity.com. [online] Available at: https://terranovasecurity.com/blog/transparency-after-data-breach/

Information Commissioner's Office. (2024). Accountability and governance. [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/.

Sanderson, R. (2011). A secure data protection strategy. Network Security, 2011(3), pp.10–12. doi: https://doi.org/10.1016/s1353-4858(11)70025-3.

Shaunessy, P. (2023) What is a permitted use of data clause? Zuva. Available at: https://zuva.ai/contract-central/permitted-use-of-data/#:~:text=Permitted%20use%20of%20data%20clauses%20are%20typically%20found%20in%20contracts,relating%20to%20data%20protection%20that [Accessed: 21 January 2024]