



LEGAL TAKE

WHY IS DATA GOLD?



Alfred Nyaga
Paralegal

INTRODUCTION

Data is often referred to as "gold" or "oil" in this age of technology because of its high value and potential for generating insights, driving decision-making, fueling innovation, generating revenue, and gaining a competitive market advantage.

Organizations that effectively harness and leverage data can gain valuable insights, make informed decisions, and stay ahead in today's highly competitive business landscape. As such, organizations ought to put in place measures geared towards ensuring data protection.

WHY IS DATA CONSIDERED VALUABLE?

1. Data fuels innovation

Data provides the raw material for innovation and can be used to develop new products, services, and business models. By analyzing data, businesses can identify patterns, trends, and customer preferences that can drive innovation and enable them to stay ahead of the competition.

2. Data drives informed decision-making

Data enables businesses to make informed decisions based on evidence and insights rather than relying solely on intuition or guesswork. Data-driven decision-making allows for more accuracy, efficiency, and effectiveness in business operations, marketing strategies, and customer engagement, leading to improved outcomes and better business performance.

3. Personalization and customer experience

Data allows businesses to understand their customers better and deliver personalized experiences. By analyzing customer data, businesses can gain insights into customer preferences, behavior, and needs, which can be used to tailor products, services, and marketing campaigns to individual customers. This personalized approach can enhance customer satisfaction, loyalty, and retention.

4. Business optimization and efficiency

Data can be used to optimize business operations and processes. By analyzing data on key metrics such as operational performance, supply chain management, employee productivity, businesses can identify areas for improvement, reduce costs, and enhance efficiency. Data-driven insights can also help in identifying and addressing bottlenecks, risks, and bottlenecks in business operations.

5. Revenue generation

Data can be leveraged to generate revenue through various means, such as data monetization, targeted advertising, and cross-selling or upselling opportunities. By analyzing data, businesses can identify revenue streams, optimize pricing strategies, and develop new business models based on data-driven insights.

HOW IS DATA ABUSED OR MISUSED?

Considering the value of information highlighted above, how can malicious individuals or organizations misuse or abuse information?

- *Data breaches*

Data breaches occur when unauthorized individuals gain access to data, such as personal information, financial data. Such unauthorized access can result in misuse of data, such as identity theft or fraud. Data breaches can have severe consequences for individuals and businesses, including reputational damage, financial losses, and legal liabilities.

- *Data misuse by employees*

Employees with authorized access to data may misuse it for personal gain, such as for financial fraud, insider trading, or other unethical purposes. This can result in breaches of trust, financial losses, and legal consequences for the organization.

- *Discriminatory use of data*

We have seen instances of data being used to discriminate against certain individuals or groups based on their race, gender, religion, or other protected characteristics. An example of this is the integration of softwares by lenders to determine credit scores of individuals. This can result in unfair treatment, bias, and perpetuation of social inequalities.

- *Data phishing and cyber attacks attacks*

Phishing attacks result where individuals are tricked into providing their personal information or login credentials to malicious actors. Social engineering attacks involve manipulating individuals to disclose sensitive data, such as passwords or financial information, through psychological manipulation or deception.

- *Profiling and surveillance*

Data can be used for collecting and analyzing data on individuals' behaviors, preferences, and activities to create detailed profiles or track their movements, actions, and communications. This is a gross violation of privacy, and many first world governments have been criticized for the misuse of data for this purpose.

WHY IS DATA PROTECTION IMPORTANT?

The importance of data protection increases as the amount of data created and stored by organizations intensifies. Therefore, with the advancements in tech infrastructure, many organizations are embracing online transactions and e-commerce to boost their business. As such, there is a lot of movement of data which is susceptible to risks such as data breaches, unauthorized access, misplacements, and cyberattacks which involve theft of the company information to commit acts of fraud or even sell the information to other people.

Data protection measures prevent organizations and individuals' data from fraudulent activities, hacking, scams, phishing, identity theft among other data security concerns.

Further, unauthorized data access of client data causes reputational harm on organizations. Such reputational hits can result to drop in sales and loss of potential customers and clients who no longer have confidence in sharing their personal sensitive information to the organization.

Organizations can also suffer heavy fines, penalties, and sanctions from regulatory bodies such as ODPC for not complying with data privacy laws in Kenya.

In turn, this can cost the organization a significant amount of money which can even lead to financial constraints on the company.

In view of the foregoing, organizations need to ensure the safety of the information they collect and store by implementing data protection measures. This is by ensuring that the company is compliant with data protection regulations.

WHAT DATA PROTECTION MEASURES CAN ORGANIZATIONS PUT IN PLACE TO SECURE INFORMATION?

- (i) **Registration with the ODPC** – as the regulatory body, the law requires entities to be registered with the ODPC. This shows good faith in compliance with the laws and gives customers comfort regarding the safety of their data.
- (ii) **Technical measures** – organizations can engage data security and cyber security experts to integrate technical infrastructure to secure all data in their possession. Such measures include biometric access to physical spaces, use of anti-virus and anti-malware software, password protection and limiting employee access to certain data.
- (iii) **Legal measures** – legal experts ensure that organizations are compliant with data privacy laws through the preparation of data protection policies, non-disclosure agreements, privacy policies and means of consent.

CONCLUSION

Data can be equated to gold due to its 'economic' value.

Considering the competitive advantage that data gives to any business, it is important for all entities to consider how information is safeguarded. Therefore, the advent of robust technology in business transactions necessitates organizations to put in measures aimed at ensuring protection of data belonging to their clients to avoid disruptions of data security.

In case you require further information on this topic, please get in touch with **Alfred Nyaga** at alfred@fmcadvocates.com

PUBLISHED BY



FMC ADVOCATES

2nd Floor, Left Wing
The Crescent, Off Parklands Road
Westlands
Nairobi - Kenya
www.fmcadvocates.com

© ALL RIGHTS RESERVED

This article is for informational purposes only and does not constitute actionable legal advice.
In case you require specific advice on a matter that concerns you, please speak to a lawyer.