DATA BREACHES: MINIMISING LIABILITY

Implications of a Data Breach

A data breach or loss can be devastating to a business due to the financial and legal implications. It is not only large corporates but also medium to small businesses which are at risk with the adverse impact being felt by the latter due to limited resources. The implications of a data breach on a business can result in:

- **the loss of sales** - A breach will not only require the diversion of personnel and financial resources, but it may also result in the business being taken offline to address the breach resulting in a loss of revenue.

- **reputational loss** – The erosion of trust as a result of a data breach or loss, and the potential negative publicity can slow or extinguish the growth prospects of a business.

- **business disruption** – Data breaches can result in the slowing down or on the further spectrum, the shutting down of the IT infrastructure for remedial action to be undertaken which, can take days or months to resolve. Ultimately, the direct and indirect financial implications of such remedial action will impact the bottom line of a business.

- **the potential closure of a business** – The costs associated with a data breach, such as procuring specialist services to assess the data breach up to and including penalties and settlements, can result in a company becoming insolvent. An example is the case of Retrieval-Master Creditors Bureau Inc. (RMCA), the parent company of American Medical Collection Agency (AMCA), a US debt collection company, which was hacked resulting the in loss of data of about 25 million people. Due to the costs of procuring consulting services, notifying data subjects, the resultant legal claims, and the disruption of AMCA's business, RMCA filed for bankruptcy protection under Chapter 11 of the United States Bankruptcy Code.

- **Administrative sanctions and legal actions** - In Kenya, the Data Protection Act, 2019 (the "**Data Protection Act**") provides for administrative fines of up to KShs 5 million, or in the case of a business, up to 1% of its annual turnover of the preceding financial year, whichever is lower. Kenyan businesses also need to be aware of the extraterritorial application of the laws relating to data protection which can result in administrative fines being imposed by foreign authorities. For example, the European Union's (EU) General Data Protection Regulation (GDPR), which protects the data of EU citizens, can fine businesses providing goods or services to individuals who are in the EU that have breached the GDPR, with fines up to €20 million, or in the case of a business, up to 4% of its total global turnover of the preceding fiscal year, whichever is higher. In such an instance, a business might also face potential claims being lodged both locally and abroad

by data subjects, with the potential liability of the business running into millions of dollars.

Mitigating Risk

1. ***Data Mapping***

Data Guard, a UK compliance and security software company describes data mapping as *"a method of documenting the information flow inside and outside an organisation, including the types of data collected, their purpose, and the locations of storage and processing facilities."* In our article, *Data Protection Act 2019 - Data Protection Series: Data Mapping*, we highlight the statutory requirement for data mapping and its importance for businesses in Kenya. We also provide a list of questions to guide data processors and data controllers when undertaking a data mapping exercise.

Data mapping greatly helps data controllers to identify data and how such data is interlaced with the business's data privacy compliance requirements. Failure to undertake such an exercise exposes a business to a data breach risk given that the IT security in place might not protect the relevant data, and it limits a business's control over the management of access to personal data. An example of such an occurrence is the Marriot data breach relating to the hotel chain Marriot's Starwood brands which was acquired in 2016 but whose network had been breached in 2014 while Starwood was a separate company. The data breach was identified in 2018, and this failure by Marriot to perform adequate due diligence to safeguard their system with a stronger data loss prevention strategy resulted in Marriot being fined $123 million.

2. ***Data Protection Compliance***

Ignorance or mistake in the implementation of a data loss prevention strategy are not defences to the protection of privacy. Businesses should therefore prioritize compliance with the Data Protection Act and put in place systems aligned with the requirements and guidelines to mitigate the risk of data breaches. A case study of failure to comply with data protection regulations is the British Airways breach that resulted in the airline being initially fined by the UK's Information Commissioner's Office (ICO) £183 million which was reduced to £20 million. According to the ICO, the data breach would have been prevented if British Airways had put in place sufficient security measures to avoid the breach of the personal data of nearly 500,000 individuals.

3. ***Cyber Security***

According to the World Economic Forum's *Global Risks Report 2022*, businesses are currently operating in a world in which "*…95% of cybersecurity issues can be traced to human error and where insider threats (intentional or accidental) represent 43% of all breaches."* Businesses, therefore, need to invest in cybersecurity, adequate IT infrastructure and put in place clear cybersecurity policies and procedures to regulate access to personal data by only authorised persons. As demonstrated above in the British Airways breach, failure to have appropriate technical and organisational measures can result in serious financial consequences. Recently, Absa Bank in Kenya had been ordered to pay by the High Court of Kenya KShs 1.5 billion (approximately $15 million) for a data leak. The disclosure by the lender's officers of financial data without authority or consent reflects the type of risks associated with a human component in any prevention system.

4. Cyber Insurance

In 2021, it is stated in the Interpol *African Cyberthreat Assessment Report* that Kenya had 72 million threat detections of ransomware and business email compromise attempts. Cybercriminals target systems that lack security, but this does not deter them from targeting large corporations that have the financial resources to instal sophisticated IT security systems. As such, it is prudent for businesses to procure cyber security insurance to cover liability resulting from a data breach more so if they are dealing with sensitive personal data. The more digitally integrated a business is, the greater importance that such a cover is procured.

The Office of Data Protection Commissioner (ODPC) is yet to publish any guidelines on the considerations to be made when levying penalties. Clarity on this issue might be on the horizon with the ODPC investigating 40 digital credit providers for misuse of personal data. It remains to be seen whether they will issue guidelines like those under review in the UK that set out various considerations in the calculation of penalties. That notwithstanding, if a business is heavy in data, it should have already started its data protection compliance, and if not, it should start today to mitigate data breach or data loss risks.