

Reports & Insights series

DATA PROTECTION &
CORPORATE GOVERNANCE

Prepared by:
Stephanie Kioko



Disclaimer

This legal alert is prepared for informational purposes only and does not constitute legal or other advice. You should therefore not take, or refrain from taking action based on its contents. This legal alert is also not intended to create, and receipt of it does not constitute, an advocate-client relationship.

According to the OECD Principles of Corporate Governance, Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of accomplishing those objectives and monitoring performance are determined.

Boards of Directors on a worldwide scale are grappling with issues concerning the increasing risk of cybercrime, IT security and unauthorized access to data and information. How do these boards stay abreast with the numerous technological advancements while still having systems that protect data? Unfortunately, companies have had to play catch up and mitigate the risks long after the data breaches have occurred.

In implementing a corporate governance framework, boards should have it as robust as possible and include risk management as a core part. Data Protection is principally about processes, IT infrastructure and the people who have authorized access to use or transfer data. In building this framework in regards to Data Protection, the organization should ideally follow these steps. The same could be referred to as a Data Protection Impact Assessment.

The evaluation of current data held by the company comes in first. The principles of personal data protection require that the data should be collected for a legitimate purpose and the purpose of which is communicated to the data subject. Data collected should be relevant and adequate, nothing in excess of what is required by the organization. Accuracy is fundamental and should be kept up to date. The data subject further has the right to have inaccurate data erased and rectified without delay. Lastly, an organization should only keep data for a period in which it is necessary. Flowing from this, organizations need to do a deep dive and find out what kind of data they hold and if it is necessary and abides to the principles of data collection.

Secondly, what kind of IT infrastructure does the company hold? Is it sufficient to process all the data collected and stored? How well does the organization anticipate and mitigate problems such as complete system failures, disaster recovery, data breaches? Companies should be able to aptly identify the present gaps in their current infrastructure. Organizations are progressively moving towards cloud-based solutions to mitigate such risks.

Lastly, we have to remember that people will always be at the center of all of technology. We develop and implement the tech solution. Regardless of how much technology advances, it will never replace human beings in totality. Certain safety measures need to be put in place to ensure that access to data being handled by people in the organization is authorized and protected. First and foremost, there should be a controlled limit to the access points by using physical biometric solutions such as face recognition, fingerprint, hand geometry and iris recognition. Organization can also use end to end encryption. This is important because in the unlikely event that data has been unlawfully obtained, it will not be accessible by the culprit. Use of two level authentication, token encryption and smart cards may also help in lessening exposure.

Data protection as an element in Corporate Governance should now be embraced by organizations. Boards are definitely the drivers of this vehicle. They should place the organizations where data is protected and risks are mitigated efficiently. The absence of this may lead in the loss of funds while defending suits, compensating victims and paying huge fines. As Kenya, I hope we move in speed as technology waits for no man.