Lawyers Hub Kenya
ACK Garden House , 1st Ngong Avenue,
Bishops Road.
P.O. Box 2468 - 00621.
Nairobi, Kenya
info@lawyershub. ke
+254784840228

The Kenya Data Protection Act, 2019

Data Protection and Know Your Customer (KYC) Implications

Introduction

The much-awaited Data Protection Bill 2019 was signed into law by the President on **Friday, 8th November 2019.** This follows a long legislation process from 2012, that at one time saw two Versions of the Bill in the Senate and the National Assembly.

The main object of the Act is to **give effect to the Right to Privacy under Article 31 (c) and (d**), establish the office of the Data protection Commission, make provision for regulation of processing of personal data and provide for rights of the Data subjects and obligations for data controllers and processors.

This could not have been more timely, as Kenya steers itself to harness the potential of the digital economy, through its Digital Economy footprint. The footprint recognizes the place of digital technologies -in promoting financial inclusion and sound data protection Law as an enabler to achieve this end.

Know Your Customer (KYC)

Financial markets must always deal with the risk of money laundering activities. Money laundering basically involves wide range of activities intended to obscure source of illegally obtained money to create the appearance that it has been derived from a legitimate source.
The process involves 3 stages:

- **Placement**- introduction of illegally obtained money into the financial system
- **Layering**- separation of illicit money from their source through a series of complex layers of transactions to disguise the audit trail.
- **Integration**- where the layering process succeeds, the integration process places back the money into the economy as legitimate funds.

Clearly, money laundering comprises the integrity of any financial system and paves way for financing of illegal activities such as terrorism and trade in weapons of mass destruction.

KYC intends to ensure integrity in financial markets by requiring institutions to properly establish the identity of their clients.

Financial Institutions

Financial institutions have a general obligation under the *Proceeds of Crime and Anti Money Laundering Act 2009*, to establish measures to verify the identity of their customers and maintain adequate customer records including those of their transactions.

Pursuant to this, several regulators such as the Central Bank of Kenya (CBK) and the Insurance Regulatory Authority (IRA) have established guidelines to help their licensees comply with this requirement.

To begin with, CBK mandates that identity of customers must be verified when[1] :

a) establishing initial business relations
b) undertaking occasional or one-off transactions

1. Guidelines on Proceeds of Crime and Money Laundering (Prevention) CBK/PG/08

c) When there is cause to be suspicious
d) When there is doubt about veracity or adequacy of previously obtained customer identification information

The Data Protection Act (DPA) of 2019 however requires that all these legislations comply with the principles of Data Protection set out in the Act.

These principles include l**awful processing, data minimization, purpose limitation**
accuracy, adequacy and relevance.

The Central Depository System (CDS) facilitates the dealing of securities in an electronic form through book entry transactions. This dispenses the need to use physical share certificates which can be lost or torn.
A company issuing securities in the CD may require a list of any depositor (person who holds a security account with the CD) whose account is credited with the shares of the issuer. This list will contain information such as name and ID or Passport Number of the depositor and in line with KYC requirements is meant to identify the Customer.

The Act however requires this collection be done in line with the DPA 2019.

This means the information collected **must only be that which is necessary for identification, minimal as possible and kept as long as required by law.** This further means the depository will be required to ensure the data is relevant and up to date.

The same is required for processing of information by other financial institutions such as the Capital Markets Authority (CMA). This is the body that regulates Capital Markets and sets corporate governance regulations for the industry.

Financial institutions are however exempted from complying with these data protection principles where disclosures are permitted by Law or necessary for national security or public interest.

An example is where the law permits disclosures by a Central Depository Agent of information of a depositor where they are declared bankrupt or to enable the CMA to exercise any power conferred to it by Law.

Secondly, the DPA applies to both private and Public institutions. Financial institutions such as Banks may be private or public institutions but are required to conduct regular monitoring of customer transactions.

This then helps in identification of suspicious trades e.g. deposits of large amounts in dormant accounts. Financial institutions are required to report suspicious trades to the Financial Reporting Centre (FRC). The FRC will send this information to relevant supervisory bodies e.g. CMA, CBK, IRA or law enforcement agencies for further handling.

The requirements for constant monitoring may mandate them to appoint Data Protection Officer. The **Data Protection Officer** shall be responsible for ensuring they comply with DPA. They shall also facilitate capacity building of staff and advise on data processing requirements under the Law.

Third, financial institutions will be required to register as data controllers and data processors unless exempted by the Data commissioner. In order to register they will need to provide a description of the personal data they wish to collect, the reason for processing e.g. as a legal obligation to comply with KYC requirements, and any risks or safeguards they have set up to ensure protection of personal data.

Conclusion

In conclusion, the DPA 2019 introduces the requirement for financial institutions to comply with data protection principles particularly purpose limitation, data minimization when discharging their KYC obligations. This is in relation to establishing customer identity, keeping records and discharging continuous obligation of monitoring and supervision of transactions.