Reconciling Data Protection and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Obligations for NBFIs

NBFIRA/RS/AML/CFT/GUN12

NBFIRA

Non-Bank Financial Institutions Regulatory Authority

Table of Contents

1. Purpose

The purpose of this guidance is to clarify how Non-Bank Financial Institutions (NBFIs) can comply with their statutory duties, to prevent and combat money laundering, terrorism financing, and proliferation financing (ML/TF/PF) while simultaneously respecting and upholding the data protection rights of their customers as required by the Data Protection Act (DPA). It is designed to provide support to Non-Bank Financial Institutions (NBFIs) in navigating the intersection of their obligations under the Financial Intelligence Act (FIA), 2022 and the Data Protection Act (DPA), 2024. and the subsequent amendments.

2. Scope

This Guidance Note applies to institutions licenced, exempted and supervised by the Non-Bank Financial Institutions Regulatory Authority (NBFIRA) through various primary and secondary legislation. It specifies considerations for the AML/CFT programme of a regulated entity. The guidelines are not intended to be exhaustive nor to set limits on steps to be taken by regulated entities to detect, prevent and report financial crimes.

3. Associated Documents

Document	**Reference**
Data Protection Act	Act No.18 of 2024
FATF Recommendations	
Financial Intelligence Amendment Act	Cap 08:07
Financial Intelligence Act	Cap 08:07
Financial Intelligence Regulations	

4. Definitions

Term	**Definition**
Customer Due Diligence	The process where relevant information about a customer is collected and evaluated for any potential risk of commission of financial offences.
Data Subject	A natural person who is the subject of personal data
Data Protection	Data Protection refers to practices, safeguards and rules designed to protect personal and sensitive data from unauthorized access, misuse or data breaches.
Data Protection Impact Assessment	Process carried out to identify, assess and mitigate the privacy risks associated with using new technologies for data processing operations which are likely to result in high risk to the rights and freedoms of natural persons.
Enhanced Due Diligence	Refers to a higher level of due diligence required to mitigate the increased risk of commission of financial

	offence. This involves obtaining additional identifying information about customers.

5. Acronyms and Abbreviations

Abbreviation	
CDD	Customer Due Diligence
DPA	Data Protection Act
DPIAs	Data Protection Impact Assessment
FI Act	Financial Intelligence Act
FIA	Financial Intelligence Agency
FI	Financial Institution/s
IDPC	Information and Data Privacy Commissioner
KYC	Know-Your-Customer
ML	Money Laundering
NBFI	Non-Bank Financial Institution/s
NBFIRA	Non-Bank Financial Institutions Regulatory Authority
PF	Proliferation Financing
TF	Terrorism Financing

6. Responsibility

The Board of Directors or the most senior management, (where a board of directors is not present), of NBFIs are accountable and responsible for their entities' compliance with the provisions of the FI Act, DPA and all other financial services laws. The responsibility may be delegated to management to ensure compliance during day-to-day business activities as conducted by NBFI.

7. Legal Basis for Issuing This Guidance Note

NBFIRA's authority to issue this guidance note is derived from its statutory mandate under the NBFIRA Act and the FI Act.

a) **Section 53 of the NBFIRA Act, 2023** empowers the Regulatory Authority to publish a Guidance Note relating to the interpretation or application of a provision in any financial services law to provide clarity, consistency and certainty.

b) **Section 49(1)(c) of the FI Act, 2022** mandates NBFIRA as a supervisory authority to issue guidance notes, to raise awareness amongst specified parties regarding ML/TF/PF risks.

This guidance note is therefore issued in exercise of these powers to ensure that NBFIs develop and implement systems and policies that are compliant with both the letter and the spirit of the law.

7. 1 Key Principles

7.1.1 Legal Basis for Processing Personal Data:

a) The DPA, 2024 prescribes 6 legal basis for processing personal data. Furthermore, processing sensitive personal data requires additional conditions under DPA Section 30(2). NBFI's are required to demonstrate that they understand the basis on which they process personal data.

b) The FI Act, and its regulations impose a clear legal obligation on NBFIs to:

(i) Collect and verify customer identity information
(ii) Conduct customer due diligence (CDD) and enhanced due diligence (EDD)
(iii) Maintain records for a specified period (currently a minimum of 20 years from the end of a business relationship)
(iv) Report suspicious transactions and/or activities to the Financial Intelligence Agency (FIA)

The legal obligations placed on NBFIs by the FI Act forms part of a legal basis for the collection, processing, and retention of customer data for AML/CFT purposes. In the event of any conflict or inconsistency between the provisions of the FI Act and the DPA on AML/CFT or any other laws on combating the commission of financial crimes, the provisions of the FI Act shall take precedence.

7.1.2 Precedence of the FI Act:

As per Section 3 of the FI Act, in the event of any conflict or inconsistency between the provisions of the FI Act and any other law on combatting the commission of financial offences the provisions of the FI Act shall take precedence. This is a fundamental principle established to ensure the integrity of Botswana's financial system and its compliance with international standards set by the Financial Action Task Force (FATF).

7.2 Appointment of Data Protection Officer

NBFIs as data controllers and data processors have a responsibility to comply with the legal obligations of the Data Protection Act by appointing Data Protection Officers. The DPO is the main contact for data subjects, supervisory authorities and internal stakeholders on all matters related to data privacy and data protection. Contact details of the Data Protection Officer should be displayed in the premises. Customers should be informed of their rights to lodge a complaint internally or with the Information and Data Protection Commission.

7.3 Practical Guidelines for NBFIs

7.3.1 Data Minimisation and Necessity:

a) NBFIs should ensure that they collect data that is adequate, relevant and limited to what is necessary in relation to AML/CFT risk assessment and CDD obligations as required by the FI Act. The amount of data collected should be proportionate to the assessed ML/TF/PF risk associated with the customer or transaction. A risk-based approach should be applied, as detailed in NBFIRA's other AML/CFT guidance notes.

b) NBFIs are increasingly relying on advanced technologies to process personal data. Section 65 and Section 72 (2) of the Data Protection Act requires NBFIs to conduct an assessment of the impact of the envisaged processing operations on the protection of personal data taking into account the nature , scope, context and purpose of processing if it likely to result in a high risk to the rights and freedoms of natural persons.

7.3.2 Transparency and Customer Communication:

a) NBFIs should process personal data in a transparent manner in relation to the data subject. Customers should be informed about the purpose of data collection, whether the data will be shared with third parties, how long the data will be kept and how to exercise their rights under the DPA. This information should be included in customer agreements, privacy policies, and other relevant documentation. The notice should explain the legal basis for processing the personal data.

7.3.3 Data Retention:

a) NBFIs are required to retain records relating to customer identity, transactions, and business relationships for a period of 20 years after the termination of the business relationship or the date of the transaction, as stipulated by Section 32 of the FI Act.

b) The DPA's "right to erasure" or "right to be forgotten" does not apply to this data during the mandatory retention period, as the retention is a legal obligation under the FI Act.

c) Once the mandatory retention period has expired, NBFIs should have a clear policy for the secure and irreversible deletion or destruction of such data, in line with the DPA.

7.3.4 Data Subject Rights:

a) The DPA grants data subjects rights, including the right to access their personal data, the right to rectification, and the right to object to processing.

b) NBFIs must establish clear internal procedures to handle these requests.

c) While a data subject has a right to access their data, this right is not absolute. Access may be refused or restricted where it could compromise an ongoing ML/TF investigation or reveal information that could prejudice law enforcement or the national interest, in accordance with both the FI Act and the DPA.

d) NBFIs should not inform a customer that a Suspicious Transaction Report (STR) has been submitted to the FIA, as this would constitute "tipping-off," which is a criminal offence under Section 46 of the FI Act. This is a critical exception to the DPA's right to information.

e) As per Section 49 of DPA individuals have the right not to be subject to decisions made solely through automated processing, including profiling, if such decisions have legal or significant effects on them. This right does not apply when the decision is necessary for a contract, based on the individual's explicit consent, or authorized by law. In cases where exceptions apply, data controllers must implement safeguards to protect the individual's rights and interests, such as allowing human intervention, enabling the person to express their viewpoint, and providing an opportunity to contest the decision.

7.3.5 Data Security and Confidentiality:

a) Lawful data sharing is permitted under both the FI Act and the DPA; however, such sharing must be governed by formal data sharing agreements that ensure confidentiality, data security, and compliance and applicable laws. The agreement should clearly define the purpose, scope, and safeguards for data exchange between the concerned parties. Unauthorised disclosure, cross-border transfers without adequate protection, or sharing of data for non-statutory purposes is strictly prohibited.

b) NBFIs must implement robust technical and organisational security measures to protect customer data from unauthorised access, loss, or destruction, as required by both the FIA and the DPA.

c) All employees involved in processing customer data for AML/CFT purposes must be adequately trained on their confidentiality obligations and the specific legal requirements of both the FIA and the DPA.

d) Any breach of customer data must be reported to the Information and Data Protection Commission as required by the DPA.

7.4 Conclusion

NBFIs must develop a comprehensive compliance program that integrates both their AML/CFT and data protection obligations. By grounding their data processing activities for legal basis of the DPA acknowledging the precedence of the FI Act in the event of an inconsistency or a conflict in matters relating to AML/CFT, NBFIs can effectively combat financial crime while upholding the privacy rights of their customers.

It is the responsibility of each NBFI to ensure that its internal policies, procedures, and systems are aligned with the principles outlined in this guidance note.