Financial Intelligence Centre

DRAFT PUBLIC COMPLIANCE COMMUNICATION

DRAFT PUBLIC COMPLIANCE COMMUNICATION

No. 22A

GUIDANCE ON INFORMATION PROCESSING IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT 38 OF 2001, IN RELATION TO DATA PROTECTION

PCC SUMMARY

Accountable institutions, in fulfilment of their compliance obligations with the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act), are required to obtain, assess and report certain personal information in relation to their clients. These obligations as set in the FIC Act cannot be circumvented, or limited owing to data privacy protection laws. Complying with obligations set out in the FIC Act are considered to be complying with obligations imposed, required and authorised by law. Accountable institutions should, however, consider the principles set out in data privacy protection laws to ensure that they do not contravene any such laws.

The processing, analysis and escalation of information regarding personal information, as received through reporting mechanisms to the Financial Intelligence Centre (Centre), is permissible by the Centre.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the user's legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

COPYRIGHT NOTICE

OBJECTIVE

The objective of this PCC is to clarify the interplay between the collection, assessment and reporting of client's personal information in compliance with the FIC Act and data protection laws.

1. INTRODUCTION

1.1. An accountable institution must comply with the Financial Intelligence Centre Act 38 of 2001 (FIC Act) when it establishes a business relationship or conducts a single transaction with a client. Chapter 3 of the FIC Act sets out the accountable institution obligations which include but are not limited to conducting risk assessments, customer due diligence, account monitoring, scrutinising client information, reporting and record-keeping. In order to comply with the FIC Act obligations, the accountable institution is required to obtain, process and further process certain **necessary** personal information and special personal information.

1.2. The FIC Act applies in a mutually non-conflicting manner to the principles of data privacy protection laws. The FIC Act provides the necessary justification in law that accountable institutions and reporting institutions require to obtain, process and further process personal information in terms of data privacy protection laws.

2. DOMESTIC DATA PRIVACY LEGISLATION

2.1. The South African data privacy protection legislation is the Protection of Personal Information Act, 2014 (Act 4 of 2013) (POPIA). POPIA promotes the protection of personal information and special personal information processed by public and private bodies and sets conditions for obtaining, using and processing of such information.

2.2. The Centre advises that accountable institutions take note of the below considerations in understanding its FIC Act obligations in light of client privacy concerns. It is advisable to first read Guidance Note 7 for a comprehensive view of FIC Act obligations, prior to these below considerations.

Risk based approach

2.3. Accountable institutions must apply a risk-based approach to combatting money laundering, terrorist financing and proliferation financing (ML/TF/PF). The risk-based approach is founded on the principle of proportionality, the higher the ML/TF/PF risk,

the more information the accountable institution would require for customer due diligence (CDD) and ongoing due diligence (ODD).

2.4. The personal information and special personal information that the accountable institution obtains, uses and further processes must be necessary to achieve the objectives of the FIC Act. The personal and special personal information obtained about the client in terms of the FIC Act should be adequate, relevant and not excessive, for the purposes of complying with the obligations of the FIC Act, taking into account section 38 of the POPI Act. The harmony between the FIC Act and POPI Act lies in the accountable institution asking only for personal information and special personal information that is necessary to achieve the purposes of the FIC Act.

Customer due diligence

2.5. Upon establishing a business relationship or conducting a single transaction when collecting personal information or special personal information the accountable institution is advised to **inform/disclose** to the client, that the accountable institution must comply with its obligations in terms of the FIC Act, and in order to do so it has to obtain, use and further process certain personal and special personal information. Once the accountable institution has obtained the information for purposes as set out in the FIC Act, the accountable institution may then use that personal information and special personal information for processing and further processing to comply with their obligations in terms of the FIC Act.

2.6. Clients have the **freedom to choose** whether to establish a business relationship or conduct a single transaction with the accountable institution. The accountable institution should advise a client on the consequences should the client refuse to provide personal or special information, provided such information does not amount to tipping off.

2.7. Where the client does establish a business relationship or conduct a single transaction, the accountable institution must comply with its obligations in terms of the FIC Act. Where the client refuses to provide personal or special personal information

as required for purposes of complying with the FIC Act and bases the refusal on data privacy protection concerns or laws, the accountable institution:

2.7.1. May not establish a business relationship or conduct a single transaction with a client,

2.7.2. May not conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction,

2.7.3. Must terminate an existing business relationship with a client, and

2.7.4. Consider filing a report in terms of section 29 of the FIC Act.

2.8. This PCC provides an overview of the application of the FIC Act in respect of data privacy legislation for accountable institutions.

2.9. Where an accountable institution follows an approach of single client view, it is recommended that the client would be notified that their information is shared across group functions, including where this information is shared cross border. (see PCC 43 on the sharing of information).

2.10. Where required, accountable institutions should take note of section 57 and 58 of the POPI Act, and should consider application for prior authorisation where special personal information is to be transferred outside of South Africa.

Reporting

2.11. Conducting certain obligations in terms of the FIC Act amounts to processing in terms of the POPIA, for example filing section 28, 28A and 29 of the FIC Act reports with the Centre. The filing of reports as processing of personal/special personal information is justified as it is an obligation imposed by the FIC Act.

2.12. An accountable institution may not disclose information relating to a report filed through to the Centre in terms of section 28, section 28A and section 29 of the FIC Act (unless as provided for in law), and further the accountable institution may not disclose information relating to requests for information in terms of section 27 and section 32 of the FIC Act. The disclosing of the fact that a report was submitted to the

Centre, or the content of such a report other than as provided in terms of the FIC Act is regarded as a tipping off offence in terms of the FIC Act (section 29(4)).

2.13. The accountable institution can collect personal information from a third party where compliance with the requirement to collect directly from the client or other persons would prejudice the lawful purpose of the collection. There is justification for the accountable institution to obtain such further information from a third party and not directly from the client or other person, as the collection of information directly from the client may amount to tipping off.

Record-keeping

2.14. Records of personal information and special personal information being kept by the accountable institution or a third party on behalf of the accountable institution must be held for the purposes of and in accordance with the FIC Act and the Money Laundering Terrorist Financing Regulations.

2.15. Where the period as set out in the FIC Act lapses, the personal information and special personal information may not be used for purposes of the FIC Act.

Use of third parties

2.16. Accountable institutions can either obtain personal information or special personal information directly from the client or through the use of a third party (refer to PCC 12A). Where the accountable institution does obtain personal information or special personal information from a third party, the accountable institution is advised to disclose to the client that it relies on third parties for obtaining certain personal information and special personal information, (unless such disclosure would prejudice the lawful purpose of the collection disclosure is not required, as stated in paragraph 2.13. above).

3. INTERNATIONAL PRIVACY LEGISLATION AND STANDARDS

3.1. Any restrictions in terms of international privacy legislation or standards does not exempt an accountable institution from complying with their obligations in terms of the FIC Act.

3.2. Accountable institutions are advised to determine whether the data privacy legislation provides for the collection, usage and further processing of data when required in terms of law, as the FIC Act provides the legal justification upon which accountable institutions collect, use and further process personal information.

3.3. Sharing of information across a group allows for effective ML/TF/PF risk identification, mitigation, and management. Further, it enables enhanced screening and monitoring of transactional activity for suspicious and unusual transactions.

4 CONSULTATION

4.1 Before issuing guidance to accountable institutions, supervisory bodies and other persons regarding their performance, duties and obligations in terms of the FIC Act or any directive made in terms of the FIC Act, the Centre must in accordance with section 42B of the FIC Act—

4.1.1 Publish a draft of the guidance by appropriate means of publication and invite submissions

4.1.2 Consider submissions received.

4.2 Commentators are invited to comment on the draft guidance by submitting written comments via the online comments submission link only, CLICK HERE. Any questions or requests relating to this draft PCC 22A may be sent to the FIC only at **consult@fic.gov.za**. Submissions will be received until **Tuesday, 26 July 2022** by close of business.

5 COMMUNICATION WITH THE CENTRE

5.1 The Centre has a dedicated compliance contact centre geared to assist accountable institutions to understand their registration obligations in terms of the FIC Act. Please call the compliance contact centre on 012 641 6000 and select option 1.

5.2 Compliance queries may also be submitted online by clicking on: http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx or visiting the Centre's website and submitting an online compliance query.

Issued By:

The Director

Financial Intelligence Centre

5 July 2022

Annexure A

Definition of personal information per POPIA, see https://www.justice.gov.za/inforeg/

Personal information

This means information relating to an identifiable, living, natural person and where it is applicable, an identifiable existing juristic person including but not limited to:

a) *Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical, or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of person.*
b) *Information relating to the education or the medial, financial criminal or employment history of the person.*
c) *Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person.*
d) *The biometric information of the person.*
e) *The persons opinions, views or preferences of the person.*
f) *Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.*
g) *The views of opinions of another individual about the person. And*
h) *The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.*

Annexure B

Definition of special personal information per POPIA, see https://www.justice.gov.za/inforeg/

Special personal information includes:

a) The religious or philosophical; beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject or

b) The criminal behaviour of a data subject of any to the extent that such information relates to:

i) The alleged commission by a data subject of any offence, or

ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.