REGULATORY

Code of conduct of the Banking Association of South Africa: What we know

2 February 2022 *10 min read*

Codes of conduct focused on the processing of personal information

by Ahmore Burger-Smidt, Director and Head of Data Privacy and Cybercrime Practice and member of the Competition Law Practice and Nyiko Mathebula, Candidate Attorney

With the Protection of Personal Information Act 4 of 2013 ("**POPIA**") in full effect it makes sense why more companies and industry associations are starting to develop codes of conduct focused on the processing of personal information.

A code of conduct provides clarity on how the conditions for lawful processing of personal information are to be applied and complied with given the features and functions of a relevant body. It further promotes a collective paradigm shift in a relevant body relating to the lawful processing of personal information.

On 20 December 2021, the Information Regulator of South Africa ("**Information Regulator**") gave notice to the public that it was in receipt of a code of conduct from the Banking Association of South Africa ("**BASA**"). The code of conduct deals with how personal information will be processed in the banking sector and aims to –

- promote appropriate practices by members of BASA governing the processing of personal information in terms of POPIA;
- encourage the establishment of appropriate agreements dealing with processing personal information as required by POPIA between members of BASA and third parties; and
- establish procedures for members of BASA to be guided in their interpretation of principally POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against banks to be considered and remedial action, where appropriate, to be taken.

This serves as a significant undertaking by BASA and its member banks given the volume of personal information processed by banks along with the sensitivity thereof. It not only goes as far as the personal details of individuals and companies such as their names, physical addresses and bank accounts, but also information pertaining to their creditworthiness, unique identifiers and the use of information matching programmes all of which are afforded special protection under POPIA.

Data privacy meets competition law: A new dawn for the regulators – find out more.

Eight conditions for lawful processing

BASA's proposed code of conduct acknowledges the importance of the abovementioned issues and deals with each, including the eight conditions for lawful processing. Some of the standout provisions are as follows:

1. General

The member banks will ensure that people, processes, technology, and organisational controls are implemented to protect the confidentiality, integrity, and availability of personal information throughout its lifecycle. Industry standards may include, but are not limited to, the Payment Card Industry Data Security Standard ("**PCI DSS**"). The PCI DSS is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

The above demonstrates a level of commitment by BASA's member banks to ensuring adequate security safeguards as required by section 19 of POPIA. This section provides that responsible parties must ensure that security measures, processes and procedures are in place (both technical and organisational) to protect against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to personal information.

2. Special Personal Information

Member banks will process the health information of their respective employees, which information constitutes special personal information, for the purposes of complying with the Employment Equity Act, 55 of 1998 and the Broad Based Black Economic Empowerment Act, 53 of 2003.

They will also process information related to criminal behaviour to the extent that such relates to the alleged commission by the relevant data subject of any offence or any proceedings in respect of any offence allegedly committed by the data subject. The extent thereof will include reporting and filing cases with the Southern African Fraud Prevention Service ("**SAFPS**") which is a non-profit company committed to combatting fraud across the financial services industry.

Information concerning race or ethnic origin may be processed by member banks in accordance with applicable laws, including but not limited to –

- The Home Loans and Mortgage Disclosure Act, 63 of 2002;
- The Broad Based Black Economic Empowerment Act, 53 of 2003; and
- Labour legislation which contains provisions regarding the employment of people who have disabilities.

Member banks will process a data subject's biometric information to verify the data subject's identity online for the purposes of establishing a relationship or processing a financial transaction. This process is also supported by the Financial Intelligence Centre Act, 38 0f 2001 ("**FICA**"). Facial recognition is also used to prevent fraud and other crimes by identifying the data subject and verifying who they are.

The above provisions are interesting to note because unless a general authorisation, alternatively a specific authorisation relating to the different types of special personal information is obtained, the banks will be prohibited from processing such information.

3. The Personal Information of Children

Member banks will process the personal information of children in limited circumstances. One such example is in the opening and managing of accounts of minors where a minor over the age of 16 and under the age of 18 who is not emancipated or married will be allowed to make a deposit at a bank without requiring the consent or assistance of a competent person. This allows the minor to execute all necessary documents, give all necessary acquittances and cede, pledge, borrow against, and generally deal with, that minor's deposit as the minor thinks fit. It also allows the minor to enjoy all the privileges and be liable to all the obligations and conditions applicable to depositors.

Section 34 of POPIA provides a prohibition on the processing of personal information relating to children unless –

- a competent person provides prior consent;
- the processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- it is necessary to comply with an obligation of international public law;
- it is for historical, statistical research purposes;
- it concerns personal information which has been deliberately made public by the child with the consent of a competent person.

Considering the above, it will be interesting to see how BASA reconciles the strict requirements of POPIA with its approach to processing the personal information of children. It seems as though consent may be the most viable avenue for the banks to consider, failing which authorisation from the Information Regulator would be required.

4. Automated Decision-Making

Member banks make use of automated decision making to provide a profile of a data subject, including their performance at work, their creditworthiness, location, health, reliability, personal preferences, or conduct. The code of conduct imposes an undertaking on the banks to ensure that data subjects are informed of their rights in respect of automated decision making. Data subjects will also have the ability to make representations about an automated decision as well as make use of the complaints procedures.

5. Information Matching Programmes

Members banks of BASA will make use of information matching programmes under the code of conduct to comply with the Financial Intelligence Centre Act, 38 of 2001 ("**FICA**"). POPIA defines this as –

> *"…the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject."*

Banks are required to conduct customer due diligence ("**CDD**") and screen customers against watch lists and may request the assistance of other banks to provide them with CDD information and/or documentation in relation to shared customers for the purposes of establishing and verifying the identity of customers.

6. Prior Authorisation

BASA's member banks will, in terms of the code of conduct, be exempt from requesting prior authorisation as contemplated in section 57 of POPIA. In particular, member banks may process –

- any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection and with the aim of linking the information together with information processed by other responsible parties such as a data subject's bank account number;
- information on criminal behaviour or unlawful or objectionable conduct on behalf of third parties where processing is on behalf of other companies which are also accountable institutions as contemplated under the Financial Intelligence Centre Act, 38 of 2000 ("**FICA**");
- information for the purposes of credit reporting given that member banks are also members of the South African Credit and Risk Reporting Agency; and
- the transfer of special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

Should this exemption be passed, it will be interesting to see how banks proceed with processing activities that would have otherwise required prior authorisation.

7. Transborder Information Flows

Banks may transfer the personal information of a data subject to a third party who is in a foreign country where such is necessary for the performance of an agreement between the relevant bank and the data subject. For example, instances where –

- the data subject uses their credit card in a foreign country to make purchases;
- the data subject has a foreign currency account and instructs the bank to transfer money to that account; and
- the data subject is party to an agreement with a lender/s and/or counterparty/ies that is/are domiciled in a foreign country.

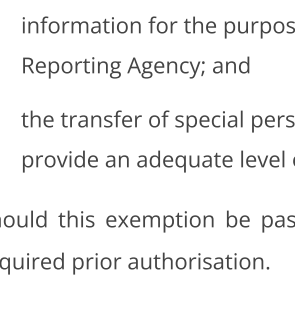
This appears to be in line with the requirements of section 72 of POPIA which deals with transborder information flows. It also accords with the nature of financial services which is fluid and often transcends national borders so it would be safe to say that a particular focus and careful application of the legislation would be required in the banking sector.

8. Dispute Resolution

Complainants are directed to first raise their issues with the relevant responsible party in accordance with the complaints management framework of the member banks. No charge will be imposed on complainants.

Complaints can also be escalated to the office of the Ombudsman for Banking Services or an independent adjudicator. Where an independent adjudicator is appointed, that person will be required to provide an annual report to the Information Regulator detailing the functions they have performed under the code of conduct for that past year and the number and nature of complaints referred to them for that past year. Complaints may also be escalated or directly taken to the Information Regulator.

As the Information Regulator grows in investigation and enforcement experience it will become increasingly important for companies, industries and professional bodies alike to align their practices in terms of data protection. A code of conduct is one of the ways in which this may be achieved as demonstrated above. Consequently, it will not be a surprise to see more applications being brought to the Information Regulator for the approval and issuing of codes of conduct.



Ahmore Burger-Smidt

Head of Regulatory

View Profile