POPIA in practice

Ever wondered about conflicts of interest declarations and the Protection of Personal Information Act (POPIA) where Employees have business interests outside the Employer? What is in the best interest of the Employer and its Stakeholders ('Data Subjects') as per POPIA? What impact does it have on the Employer, its reputation, and its other Stakeholders?

Lisa Pienaar-De Gouveia, Risk, Legal and Compliance department at Netcash gives her insights on the key considerations to bear in mind.

Legal form

Employee entrepreneurs often choose, amongst other options, either a Sole Proprietorship or a Private Company "(Pty) Ltd" (a third party) as the vehicle for their businesses. The legal differences are set out below:

Sole Proprietorship is the simplest business entity.	**Private companies** are more sophisticated.
• The business owner is entitled to all profits. • No CIPC ('Companies and Intellectual Property Commission') company registration. • No Memorandum of Incorporation. • A sole proprietor does not enjoy limited liability as there is no separation between the assets and liabilities of the business owner and those of the business. • A sole proprietor pays taxes in his/her own name according to Personal Income Tax rates. • Summons is issued in the name of the sole proprietor when s/he decides to sue, and s/he can be sued in his/her personal capacity.	• The number of owners can range from 1 (one) to 50 (fifty). • A one-man company is a private company which has just one owner and is often referred to as an owner-managed company. • One-man companies are exempt from audit. • CIPC company registration is a requirement. • A Memorandum of Incorporation forms part of the company's formal documentation. • Annual returns must be filed with the CIPC to ensure that they are in possession of the latest company information. • Private companies are separate juristic persons to their owner(s) and enjoy limited liability, i.e., there is a separation between the assets and liabilities of the company and those of its owner(s). • Private companies are subject to corporate taxes and the owner(s) is / are subject to Personal Income Tax. • Since the private company is a separate legal entity from its owners, it can sue and may be sued.

Besides mitigating conflicts of interest risk, which is a critical component of an effective Anti-bribery and Corruption compliance programme, Data Privacy, and the Protection of Personal Information of Data Subjects came into effect on 1 July 2021 in the form of the POPIA, which further increases the regulatory compliance obligation of businesses in South Africa.

The POPIA sets out 8 conditions for lawful processing. The question is whether an Employer is breaching any of the 8 conditions for lawful processing by permitting Employee entrepreneurs (with their own business interests) access to the Employer's Clients Personal Information (PI). This is whilst the Employer is fully aware that their employee entrepreneurs do not function separately from their own business interests, in the instance of sole proprietorships and function separately from their private company businesses, therefore third-party legal entities that have access to their Client PI.

What does the POPI Act say?

- The POPIA defines a "Responsible Party" as a public or private body or any other person, which alone or in conjunction with others, determines the purpose of and means for processing personal information.
- Who are Responsible Parties? Responsible Parties includes a variety of stakeholders e.g., Employers, Suppliers, Sole Proprietors, CIPC registered company, etcetera.
- In relation to its Clients, the Employer may have elected to function as an "Operator" who processes personal information for a Responsible Party (a Client) in terms of a mandate or contract, without coming under the direct authority of that party.
- The Employer may therefore have duties and responsibilities as both Responsible Party and as an Operator.
- Employee businesses are therefore Responsible Parties in their own right. These third parties have no business relationship nor business agreement with their Employer, other than an Employment Contract nor do they have any business agreement with their Employer's Clients.

The POPIA sets out 8 (eight) conditions for lawful processing as well as the rights of Data Subjects (the Employer's Clients for purposes of this article).

1. Accountability: The Responsible Party (Employer) with specific reference to the CEO or Managing Director must ensure that the conditions for lawful processing are adhered to by the entire business.
2. Processing Limitation: PI may only be processed if the Data Subject consents to the processing and that the processing protects the legitimate interest of the Data Subject. The Responsible Party must collect the PI directly from the Data Subject.
3. Purpose Specification: The PI is collected for a specific, explicitly defined, and lawful purpose. E.g., FICA documents and banking details (which are highly privileged and confidential information).
4. Further Processing Limitation
5. Information Quality
6. Openness
7. Security Safeguards
8. Data Subject Participation: Direct participation with the Responsible Party. The Employer's Clients are unaware that they are engaging Employees with their own business interests or registered companies, who are Responsible Parties in their own right.

Rights of Data Subjects

These rights include, amongst others, the right to:

- have his / her or its PI processed in accordance with the 8 conditions for lawful processing as set out in the POPIA.
- be notified by the Responsible Party that PI about him / her / it is collected by the Responsible Party and what the information entails as set out in section 18 of the Act:

    - Type of information collected.
    - Nature or category of the information.
    - Where and how it will be used and stored.
    - Purpose for which this information is collected.
    - Source from which the information is collected when it is not collected from the Data Subject directly.
    - Responsible Party name and address. *(Does the Employer want to provide the Company details of its Employee Businesses to its Clients?)*.
    - Whether or not the supply of the information by that Data Subject is voluntary or mandatory.
    - The particular law authorising or requiring the collection of the information and the law, which makes the supply of that information mandatory.
    - The contract, which makes the supply of that information mandatory.
    - The consequences of failure to provide the information.
    - Cross border transfer of information by the Responsible Party to a third country or international organisation and the level of protection afforded by that third country or international organisation.
    - Recipient or category of recipients of the information. *(Does the Employer want to provide the Company details of its Employee Businesses to its Clients?).*
    - The right of access to and the right to rectify the information collected.
    - The right to object to the processing of PI as referred to in section 11(3); and
    - The provision of the contact details of the Information Regulator and the right to lodge a complaint with the Information Regulator.
- be notified that his / her / its PI has been accessed or acquired by an unauthorised person (Company of an Employee, due to the Client not having given consent to that specific Responsible Party to have access to his / her / its PI).

In this article, the Employer Company commits itself as follows to its Clients in its Master Agreement:

- ***The Employer Company's Operator Agreement with its Clients***

    - *"When the Employer Company functions as an Operator for its Client (which Client is a Responsible Party) in terms of the Protection of Personal Information Act No. 4 of 2013 ("POPIA"), it will only process the personal information of the Client and the Client's Customers for the purposes set out in the 'The Privacy Notice and Promotion of Access to Information Act No. 2 of 2000 ("PAIA") Manual', unless otherwise required by law or in the proper performance of its duties.*
    - *The Employer Company will not use any sub-contractors for the purpose of processing personal information of the Client's Customers, except for the sub-contractors named in the Employer Company's Privacy Notice, which may be updated, from time to time.*
    - *The Employer Company will use reasonable security measures and inform its Clients of any actual or suspected security compromise as set out in the clause dealing with ('Security').*

- *The Employer Company will maintain the confidentiality of the personal information as set out in the Confidentiality Undertaking clause below."*

- ***Confidentiality Undertaking***

  - *"Each Party agrees to hold the Confidential Information in confidence during and after the termination of this Master Agreement in a manner which is consistent with the POPIA.*
  - *Each Party agrees that unless required by law (including a subpoena, discovery demand or similar compulsory process) it will neither make the Confidential Information available to any Third Party nor use the Confidential Information for any purpose other than the performance of this Master Agreement, provided that each Party shall be entitled to disclose the Confidential Information to its professional and legal advisors and its Employees (in the latter case to the extent that the transactions contemplated in this Master Agreement and/or the Annexures are within the relevant Employees' scope of duties and/or to enable the transactions contemplated in this Master Agreement and the Annexures to be implemented).*
  - *Each Party agrees to use all reasonable efforts to ensure that the Confidential Information is not disclosed or distributed by its Employees in violation of the terms of this Master Agreement.*
  - *The Parties shall implement appropriate control measures to ensure that all Employees, agents and/or subcontractors employed and/or contracted by either Party, sign Confidentiality agreements containing, inter alia, the provisions set out above."*

Conclusion and recommendations

1. It is evident from the above that Employee entrepreneurs whether Sole Proprietors or CIPC registered businesses, are Responsible Parties in their own right. These Responsible Parties are not contracted to the Employer (except for the Employee's personal employment contract to perform a specific role in the Employer Company) or to any of the Employer Clients from a business agreement perspective and have no right to or consent from any Data Subject to view their Employer Client PI from their own business point of view.

2. Employees are authorised to fulfil specific duties in terms of their employment contract with their Employer.

3. Employee entrepreneurs however also have access to the same PI when they are wearing the hat of their own business, which could potentially be interpreted as unauthorised access, by some stakeholders: Data Subjects / Responsible Parties / Regulator, etc. but not necessarily by all, since interpretation of the law can be different for different stakeholders.

4. It is recommended that Employers have a clear policy on whether conflicts of interest by their Employees are in the best interest of their business or not. It is easier when a business does not accept conflicts of interest, but this is not always possible. The Employer must have clear guidelines on what is acceptable and what not.

5. It is further recommended that a consistent approach be followed to ensure that Employee conflicts of interest do not impact the Employer's business in any way that introduces additional risk and that similar scenarios are dealt with in a similar fashion to ensure fairness.

6. It is recommended that Employers review employment contract templates to ensure that it incorporates all required confidentiality and non-disclosure clauses as required. Good practice would be for employees to sign a fresh Code of Conduct which includes ethical behaviour and confidentiality on an annual basis.

7. Formal Conflict of Interest training and awareness is required to ensure that all Employees understand conflicts of interest and why it should be avoided. The Compliance team can include this training as part of their annual Compliance Training and Awareness plan to assist the business with their training needs. The same applies to annual refresher POPIA training.

8. It is recommended that Employers make use of the relevant Information Security Management System (ISMS) data loss and/or data sharing monitoring tools as one form of risk mitigation against unauthorised sharing of company information and PI, as well as consider the Organisational, Physical, Technical and People ISO27001 control requirements.

9. The Employer may also want to consider updating its Privacy Notice to include reference to Employees with own business interests as set out in the below example:

"Client PI may be accessed or shared with the following categories of recipients:

- *Payment processing service providers, merchants, banks, and other persons that assist with the processing of client payment instructions, such as Payment Clearing House Systems Operators;*
- *Cloud-based storage facilities and data centre;*
- *Credit Bureau and similar providers;*
- *Authorities and Regulatory Bodies;*
- *Business Service providers; and*
- *Employees who assist clients during onboarding and throughout their relationship with the Company, who have business interest external to that of the Company, which Employees have attested to having read, understood, and abiding to internal Privacy and Confidentiality policies."*