POPIA to PANIC

kinetix
SOFTWARE SERVICES

POPIA to PANIC

Given POPIA's infancy and the number of entities seeking compliance, it is understandable that existing resources are limited, constrained and, very likely, expensive. This will certainly bring about a state of panic.

Besides information being ever more pervasive, an enterprise's need to create and maintain value is made that much more challenging with the rapid evolution of disruptive technology. The rate and pace of change bring about new risk and sometimes diminish existing capabilities to contain and manage the risk.

This is further impacted by the inherently sensitive nature of personal information and the additional requirements for protection it attracts. The case for responding to legislation should not only be driven by the need to achieve compliance. Risk mitigation, subsequent controls enhancement, audit assurance and opportunities for continuous improvement will certainly be value-driven consequences of an effective and ongoing privacy programme.

For most who have yet to start, what is the task at hand?

POPIA: END-TO-END COVERAGE

Privacy issues affect the entire organisation. Regardless of the operation, it is vital that all privacy- impacted processes and all stakeholders, internal and external, local or global, be identified and the stakeholders' respective responsibilities be communicated, understood and enforced.

ENABLEMENT

In any South African enterprise's pursuit of its principle to operate within the bounds of legislative and regulatory demands, it must also look to the principles established in POPIA. South Africa's newly introduced privacy legislation is based on the 8 core privacy protection principles found in legislation within jurisdictions such as the European Union (EU) and the Organisation for Economic Co-operation and Development (OECD). Clearly, it is imperative that the organisation's executive must define and uphold a data privacy policy that covers all the requirements of the legislation. This is crucial to the organisation's identification of all stakeholders as well as its understanding of the intent and direction towards the successful deployment and ongoing management and maintenance of its privacy programme.

Supporting the policy should be a code of conduct, standards, practices, procedures, rules and other policies that cover elements such as information classification, labelling, handling and protection, and clear guidelines as to the acceptable use of digital assets. Agreements between the company and any operators or processors must clearly define roles and responsibilities, rights to audit or assess, and consequences for non-compliance. Binding corporate rules are essential to communicating the data privacy policy's intent and direction across divisions of a South African-based multinational.

ORGANISATIONAL STRUCTURES

POPIA defines an information officer as being the head of any organisation. (Not to be confused with the Chief Information Officer, typically an IT-facing role). He or she is ultimately accountable for the organisation's compliance. Of course, deputy information officers may be appointed.

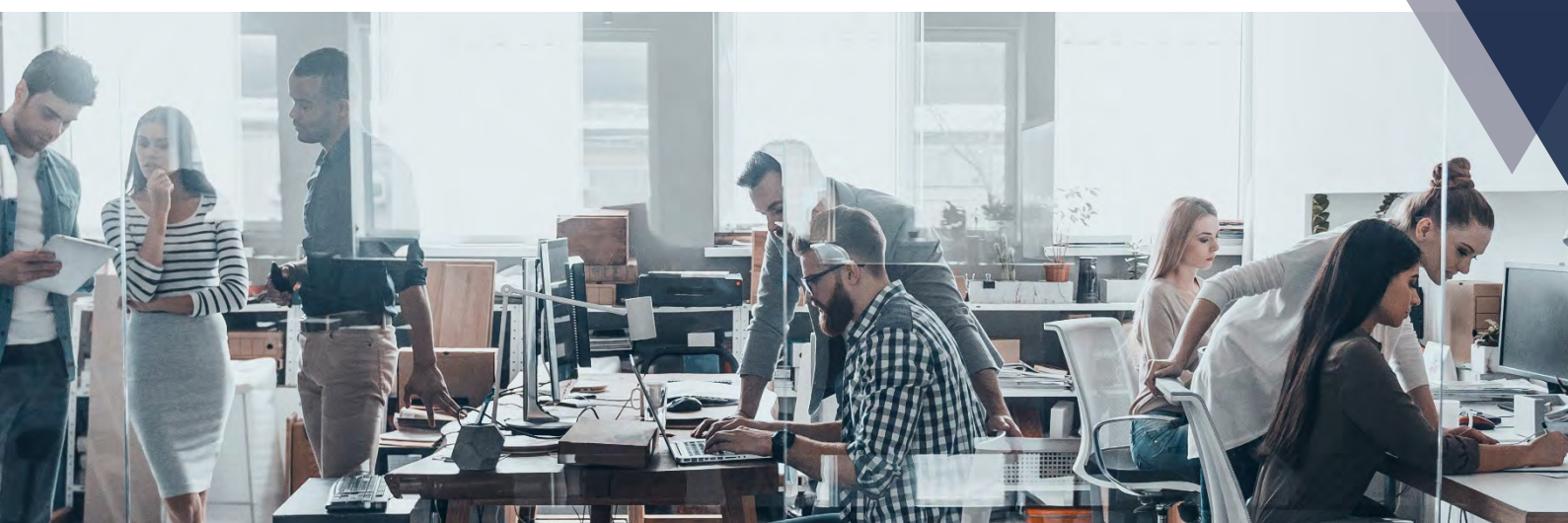
When developing a Responsible-Accountable-Consulted-Informed (RACI) chart, top-down, bottom-up, internal-external and local-global are the dimensions to be considered.

External stakeholders include the Information Regulator and all data subjects, suppliers and outsourced partners. Internally, information owners such as a sales manager or an HR director are specifically responsible for the appropriate access to and classification, integrity and handling of information of their respective data subjects, i.e., customers and employees. IT is specifically responsible for information custodianship.

These responsibilities cut across the information life cycle from collection and usage to storage and eventual demise. Employees who might be tasked with using personal information also have a duty of care. The heads of legal, internal control and business security must ensure that the management of privacy risk and assurance is embedded in the enterprise risk management process. Staff must understand the procedures to follow in order to facilitate a subject's data access request or in the event of a privacy breach. Responsible staff must be trained to manage breaches and subject access requests.

CULTURE AND BEHAVIOUR

As robust as technical controls may be, human behaviour is regularly identified as the weak link causing a security (and, potentially, privacy) breach. A sensitive discussion in an airport lounge, unverified meeting attendees, a lost or stolen unencrypted laptop or flash drive, a soft hack via switchboard, un-shredded confidential waste and an uncleaned whiteboard are examples of potential breach scenarios triggered by human behaviour. The executive and senior management must set the tone at the top and lead by example. Everyone is responsible—from the executive through to the person tasked with cleaning a whiteboard after meetings.



Privacy rights and expected behaviours should be embedded in a code of conduct. It is important to stay focused and have the creativity and stamina to maintain training and awareness. One way to do that, for example, is to have an annual privacy housekeeping week. It is also good practice to recognise good behaviour. A privacy programme is ongoing and not a one-time-only event.

In today's world, people easily, sometimes recklessly, and other times unknowingly give up their rights to privacy. There are big wins in getting employees to appreciate their rights as enshrined in POPIA. It should stand to reason that they would then appreciate how to handle the personal information of others when going about their normal course of business. 'Know your rights, know your responsibilities!' could be a good maxim.

SERVICES, INFRASTRUCTURE AND APPLICATIONS

Of particular concern should be the extent to which privacy-related issues and requirements are identified, embedded and managed within services, infrastructure and applications. In application development, for example, has privacy by design been considered and adopted? To what extent are outsourced service providers privacy-compliant? Are service level agreements (SLAs) optimised to reflect any privacy-related requirements? Do architecture principles embody privacy requirements? If not, could this, for example, be a reason for the pain experienced by HR in using in-house technology or systems?

SKILLS AND COMPETENCIES

The successful development, implementation and ongoing management of a privacy programme is dependent on people, skills and competencies throughout the information life cycle. These will most likely be identified in a properly planned privacy programme. Resource development and utilisation can be optimised by aligning with HR and HR processes, promoting the appropriate accreditations and participating in global privacy and information security forums.

GOVERNANCE

Given the infancy of the legislation and its partial overlap with existing legislation (see earlier examples), there is the risk that some, especially senior, stakeholders may discount the importance, urgency or essence of privacy requirements. This could be due to their knowledge of existing legislation and their assumption that POPIA is, basically, covered by existing legislation. How does the executive level effectively evaluate, direct and monitor if it starts off with this assumption? POPIA states that accountability lies with the head of the organisation. It is often too easy for the chief executive officer (CEO) to delegate responsibility without realising the implications of unclear directions to and expectations of management.

Management must ensure that it has a clear understanding of the data privacy policy requirements and must be empowered to justify, deploy and manage the resources necessary to deliver the privacy programme. As the executive will depend on reliable data for risk management and breach response, management must ensure the efficient deployment and maintenance of the privacy programme.

PRE-CONCEPTION

Given a decade of waiting for promulgation, it is natural to expect people to have pre-conceptions of what POPIA compliance actually means. From "Our IT security is up-to-date therefore I believe that we are compliant" to, "I don't feel I need to comply because we only process our clients' email address" – (that company has 5000 clients). The risk to compliance is obvious and the sooner they dispel these notions, the better. Privacy is not security, and security is not privacy.

ACCOUNTABILITY

The Information Officer of a private body is the head of that body, responsible for enabling the framework and applying the requisite governance. While delegation of duty is acceptable, the delegation of responsibility is going to get the CEO in a whole lot of trouble. POPIA's punitive measures are tough and you don't want to be setting any precedents.

OWNER TO OWNERSHIP

The information owner has responsibility for the maintenance, use and security of personal information. After all, it's not the CIO who manages the employee contract or the sales contract. The CIO / IT is a custodian of information, not an owner of information. Direction for maintenance, use and security comes from the information owner – the HR Director and Sales Director, respectively.

LEGAL-EASE

Relative to some other privacy regulations, POPIA is a well-written and well-structured document. People shouldn't really fear it. Of course, its dependence on the Promotion of Access to Information Act, (PAIA) does introduce complexity but this too is overcome with regular practice. This does not mean to say that the 'average-Joe' could read the document on a Sunday and then start a privacy program on the Monday – on a spreadsheet. Specialist tools and knowledge are still indispensable.

WHY POPIA IN THE CLOUD?

The key features of this platform enable businesses to demonstrate the measures taken in order to maintain compliance with the South African data privacy legislation framework (other regulation frameworks included such as GDPR), all in a single BOX.

- BE COMPREHENSIVE IN ITS COVERAGE – no half measures, providing partial and modularised (and chargeable) services.
- BE EASY TO USE – it shouldn't require the equivalent of a science degree to maintain it. Your privacy team will quickly lose interest.
- ENABLE COLLABORATION – across the enterprise, available 24/7, and everyone gets involved.
- BE AFFORDABLE – comprehensive coverage needn't cost the earth so, compare prices and understand 'value-for-money' propositions.

SUPPORT LOCAL SOUTH AFRICAN BUSINESS – by purchasing systems that are developed and maintained in South Africa you are supporting our economy thus enabling local jobs and opportunities for people to start businesses in the compliance industry.

133 Edison Crescent, Hennopspark, Centurion
P O Box 53349, Wierdapark, 0149
Phone: 087 230 8740
www.kinetixsoftware.co.za