Compliance with the Protection of Personal Information Act (PPI Act)

The commencement date of the Protection of Personal Information Act 4 of 2013 (PPI Act) has finally been announced. The PPI Act aims to give effect to the constitutional right to privacy, which is set out by the Constitution of South Africa, by introducing measures that will ensure that personal information is processed by organisations in a fair, transparent and secure manner.

pwc

Organisations have 12 months from, 1 July 2020, to become compliant. In our experience, this won't be enough time for most large and complex organisations to become compliant.

Accelerating the implementation of the PPI Act within your organisation

Implementing the requirements of the PPI Act can be a daunting task for organisations, especially if you are starting late with your programme.

Through working with many organisations over the last number of years, we have developed a number of good practices that have successfully helped organisations accelerate the implementation of the PPI Act.

What is personal information?

The PPI Act broadly defines 'personal information' as any information that can identify an identifiable living, natural person or identifiable existing juristic person. The PPI Act is unique in the global data protection landscape in its protection of personal information of juristic entities and it will require organisations to rethink not only how it processes its employee and customer personal information, but also how it deals with personal information in its business to business engagement activities.

By adopting the following key accelerators, organisations can fast-track their PPI Act implementation:

Secure accountability with relevant executives

Accountability is critical for any privacy programme to succeed. It is important for organisations to determine their view of privacy and how they plan to comply with the regulatory requirements. Based on this, agree on a number of key objectives that can be further developed into a strategy and framework to drive the implementation project.

Allocate the Information Officer role

By default, the head of the organisation is the Information Officer. However, the PPI Act allows for this role to be delegated. Decide now who will be responsible – will it be the Compliance Officer, Head of Risk or somebody else in the organisation? Take this individual on the journey from the start.

Follow a risk-based approach

Many PPI Act programs have been derailed due to teams trying to implement the requirements of the PPI Act without considerations of their unique business context. A risk-based approach to PPI Act compliance, agreed with the Board or Steering Committee, will ensure focus remains on prioritising the most important PPI Act compliance requirements first.

Integrate with existing compliance structures

Compliance with the PPI Act requires much effort which can be saved by and much effort can be saved by integrating it into existing compliance structures and processes, such as compliance management, risk management, internal audit and audit and risk committee reporting. Without an appropriate compliance process in place, it may be challenging for organisations to drive the PPI Act in isolation.

Align with other initiatives

It is important to coordinate your PPI Act compliance initiatives with related initiatives within your organisation, particularly in areas such as cybersecurity, data classification and PCI compliance to avoid unnecessary duplication of effort and ensure alignment to business objectives.

Drive behavioural change through training and awareness

Change management is a critical part of embedding privacy into the culture of the organisation. Through training and awareness, the culture of the organisation can embrace change in how they handle data, which then results in changed behaviours.

Get help outside the organisation

Develop a risk-based and prioritised implementation plan. Look inside for skills, but reach out for assistance from professionals, such as those with multi-disciplinary teams between privacy, legal, data, advisory and cyber security specialists where you don't have the skills within your organisation.

Who does it impact?

The PPI Act impacts all South African organisations, both public and private, that collect, create, use, store, share or destroy personal information.

What happens if I do not comply?

Non-compliance with the PPI Act can have serious repercussions for organisations, their employees and their customers.

Impact on organisation

- Financial penalties
- Criminal sanctions
- Loss of revenue resulting from negative press, damaged reputation
- Losing customer trust

Impact on employee

- Disciplinary action and dismissal
- Misuse of personal data
- Private or confidential data being published

Key questions you should be asking:

1. Where do I start?
2. How can I prioritise my implementation activities to comply with the PPI Act?
3. What is the PPI Act impact for my organisation?
4. What data do I process and why?
5. Where is data stored?
6. Who do I share data with and why?
7. Is my data secure?
8. How do I maximise the value of my data in a legally compliant way?
9. Is my organisation affected by other privacy laws in countries I operate out of?

How can PwC help?

We have advised and assisted many organisations, from small enterprises to large corporates, in their PPI Act compliance journeys. Based on our experience in providing privacy advisory, legal and cyber security services to our clients we have defined a holistic framework for the management of privacy risk that is designed to enable organisations to leverage good practices that can be tailored to address each organisation's unique privacy vision and risk exposure.

Assess		Design, build and implement		Maintain
Risk analysis and data discovery	**Gap assessment and remediation roadmap**	**PPI Act programme implementation**	**PPI Act programme readiness**	**Ongoing programme operation and monitoring**
Risk analysis and data-gathering activities to gain an understanding of your PPI Act risk and data footprint (including privacy impact assessments, data inventories and data flow mapping).	Identification of gaps in your privacy capabilities and prioritisation of remediation activities.	Implementation of PPI Act programme components to remediate known compliance gaps and establish privacy management practices based on your organisation's unique environment.	Performing a readiness review of your PPI Act programme to provide you with insights on your readiness. Facilitation of data breach simulations to test your PPI Act readiness through a simulated data breach scenario.	Establishing ongoing compliance mechanisms to promote continued accountability for privacy management (including compliance risk management plans, training and awareness).
Programme Management				

Privacy training

Training is an important aspect in your PPI Act compliance journey. The likelihood of complying with the requirements of the PPI Act is very slim if the individuals in your organisation do not understand the legislation and the role they need to fulfil to ensure that the purpose of the PPI Act is carried out appropriately.

PwC provides training at two levels, for executives (owners and directors of an organisation) and for employees (including management). Training covers aspects such as the purpose of the PPI Act, insight into the key sections covered by the PPI Act and training specific to the organisation's PPI Act policy standards.

Creating trust in a digital world

Data protection is at the forefront of the minds of boards, customers, users, and regulators. How you use data in the digital economy will require you to understand the connections between business, technology, people and regulation. Using our bespoke privacy management framework, we can help you assess your privacy risks and deploy privacy transformation initiatives that resonate with your unique business priorities and risks while managing regulatory change.

For a discussion about data privacy, including the PPI Act, contact us:

Busisiwe Mathe
Partner
busisiwe.mathe@pwc.com

Yvette du Toit
Associate Director
yvette.du.toit@pwc.com

Charles Fischer
Associate Director
charles.fischer@pwc.com

Aneesa Firfiray
Senior Manager
aneesa.firfiray@pwc.com