Deloitte.
Legal

Africa | Risk Advisory | 2017

Deloitte Legal – Representing Tomorrow
Getting "Regulator Ready"

The commencement date of the Protection of Personal information Act 4 of 2013 ("POPI") is expected to be announced sometime in 2017, following which organisations could have as little as 12 months to become POPI compliant or "Regulator Ready".

Can organisations become "Regulator Ready" in a year?

In October 2016, Advocate Pansy Tlakula ("Tlakula") was, through a National Assembly recommendation, appointed by the President as the chairperson of South Africa's long-awaited Information Regulator ("**Regulator**"), with effect from 1 December 2016. In her recent media briefings, Tlakula advised that the Regulator is currently mobilising its operations so that the effective date of POPI may be officially declared, triggering the 12-month grace period for compliance with its requirements.

Tlakula has also indicated that the draft regulations to POPI currently being prepared for final review which will then be made available for public comment, and thereafter be tabled in Parliament. The Regulator is currently implementing all necessary measures to ensure its **operational readiness by 2018**. Consequently, it is imperative for all organisations handling personal information to become "**Regulatory Ready**" in the next 24 months.

Based on our experience in implementing privacy and data protection projects across a range of organisations in Africa, and taking into consideration global privacy best practice, **organisations should endeavour to become "Regulator Ready" within, at the very least, the next 18 months**. Our experience has shown potential risks and resources must be factored into any rollout plans to mitigate the risks in respect of the handling of personal information. The goal is to prevent any last minute panic, ensure that organisations budget timeously for POPI compliance programmes and initiatives, and that compliance with POPI becomes "business as usual" within an organisation's culture, processes, procedures and information governance framework. Lacking such urgency in ensuring processes are implemented to become POPI compliant, especially where shortcomings have not been quantified, can increase costs exponentially when the "grace period" nears its end. Setting up an annual budgeting cycle in review of past findings and failings creates an environment which not only addresses pain point areas, but also challenges current standards, where optimisation is required.

Previous experience has shown that becoming fully POPI compliant can be challenging, expensive and possibly unfeasible for many organisations in South Africa. However, it is nonetheless possible to initiate and implement privacy compliance measures by targeting quick wins. This ensures a proactive approach to POPI compliance initiatives.

POPI compliance should constitute a significant and all-encompassing step in every organisation's data management campaign – especially where the collection, processing, storing or sharing of personal information is involved.

The **first step** that all organisations need to take in order to achieve their POPI compliance objectives, is to design a **one to three-year privacy or POPI compliance implementation plan**. There are also numerous efficient and cost effective "quick wins" which organisations could initiate and implement to commence their journey to being "Regulator Ready" and demonstrate compliance with POPI, from a data management perspective. These quick wins should ideally be initiated within an organisation's high-risk areas as far as personal information is concerned.

The Business Rationale for Becoming "Regulator Ready"

In a technologically advanced world where commerce is dependent on the free flow of information, including personal information, it is imperative that organisations become "Regulator Ready" sooner rather than later. A lack of data protection compliance would not only hinder an organisation's privacy compliance efforts with legislation such as POPI or the European Union's ("EU") General Data Protection Regulation, but would also hinder the organisation's commercial and operational footprint, as numerous jurisdictions may prohibit the transfer of personal information cross-border to other jurisdictions with inadequate data protection legislation.

Countries which **prohibit the transfer of personal information to jurisdictions with inadequate levels of data protection** include, but are not limited to:

- All countries belonging to the EU (which may also include those countries that do not belong to the EU)
- United Arab Emirates;
- United Kingdom;
- Qatar; and
- Many African countries including Angola, Ghana, Ivory Coast, Mauritius and Morocco.

The benefits of being "Regulator Ready" include:

- Augmenting an organisation's customer and stakeholder relationships;
- Enhancing confidence and transparency in the organisation's brand;
- Ensuring trust in the organisation's brand while simultaneously guarding against reputational risk;
- Enhanced data security, including protection against cyber-attacks such as ransomware and denial of service;
- Improving market competitiveness in that an organisation is more likely to be trusted by all its stakeholders if they trust that their personal information will be secure with the organisation; and
- Enhancing the organisation's overall quality of information as well as business management.

Being "Regulator Ready" is a driver for overall business growth and sustainability regardless of the industry or sector within which an organisation operates.

The failure by any organisation to be "Regulator Ready" timeously constitutes a slippery slope towards non-compliance with POPI. The risk of non-compliance could potentially attract fines from the Regulator of up to R10 million per breach, or the imposition of imprisonment for a period not exceeding 10 years, depending on the level of non-compliance. Furthermore, such a fine and/or imprisonment may consequently be accompanied by diminished profits due to the loss of customer, investor and overall stakeholder confidence as well as any protracted law suits. This has already been seen in jurisdictions with mature data privacy regulation such as in the United Kingdom ("**UK**"), where a 2015 survey found that 90% of large organisations and 74% of small to medium size enterprises had reported data breaches, which attracted the imposition of fines from the UK Information Commissioner of up to £1.4 billion (approximately R23 billion). Similarly, in 2013, a data breach which is estimated to have affected almost half a million customers saw technology giant Adobe Systems handed a $1 million (approximately R13 million) fine.

Privacy quick wins to optimise efforts to getting "Regulator Ready"

Achieving privacy and POPI compliance can be a lengthy and complex process that in our experience, may take up to 3 years to effectively embed into an organisation's business operations. This may entail organisations having to commence significant adjustments to three main elements of their business operations, namely:

- people (staff);
- processes (policies and procedures); and
- technology (information systems and applications).

The **quick wins canvassed below** constitute valuable steps to be taken by any organisation on its journey to become POPI compliant:

1. Personal Information inventory

A Personal Information inventory ("**PI inventory**") is a consolidated document which indicates what personal information is collected, used and stored within an organisation. Consider the following:

- Is your organisation aware of the various categories of personal information it collects and processes?
- Does your organisation have a holistic view of where all personal information may reside? (This includes hardcopy and electronic records which may comprise personal information).
- Who does your organisation share personal information with and why?
- Having a PI Inventory in place may assist an organisation in addressing the previously mentioned pain points.

2. Governance and Data Privacy Target Operating Model

A data privacy target operating model ("**Operating Model**") provides an overview of the proposed impact of data privacy on the internal structure, roles, responsibilities and management of an organisation and its business areas. There is no standard Operating Model for data privacy compliance purposes. In this regard, the following should be considered:

- Do you have a clear understanding of how an Operating Model for sustainable data privacy compliance is meant to apply in your organisation?
- Is the Operating Model deployed, suitable for your organisation, based on your organisation's size and geographical footprint?
- Would a centralised, decentralised or hybrid structure be most suitable for data privacy governance?

3. Privacy policy

A privacy policy prescribes and defines the handling practices and obligations that staff must abide by when processing personal information. Consider the following:

- Do all staff place a high premium on the organisation's data (including personal information), which they may collect, process and share on a regular basis?
- Is your organisation's privacy vision and/or mission statement documented for internal and external stakeholders to take cognisance of?

4. Privacy incident management plan

A privacy incident management plan allows your organisation to be more proactive and less reactive in effectively dealing with any incidents involving the loss, damage or unauthorised access to the organisation's data, including personal information. Consider the following questions:

- Have any of your organisation's personnel ever inadvertently and erroneously emailed personal information to unauthorised/unintended recipients? If so, how was such a mishap dealt with?
- Has your organisation ever been a victim of a cyber-attack? Were information systems suddenly shutdown or made inaccessible?
- Is your organisation at risk of losing any of its customers', employees' or other stakeholders' financial, medical and other personal information? If so, has your organisation adequately prepared for such an incident with pre-defined steps and checkpoints?

5. Training and awareness

As with other aspects within an organisation where personnel (junior and senior) are required to be educated, this aspect is self-explanatory. Consider the following:

- Does your organisation's management and personnel understand the framework and environment within which the organisation operates, as far as personal information is concerned?
- Are personnel aware of why they should protect personal information collected and processed by the organisation?
- Do personnel understand what constitutes personal information?

Conclusion

Organisations (particularly larger organisations) which collect and process Personal Information should immediately set out to become "Regulator Ready" if they have not commenced their privacy compliance journey as yet. Data privacy/POPI compliance is now an integral part of business globally, making becoming "Regulator Ready" of paramount importance, not from a compliance perspective, but from a business perspective.

Contacts

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Mobile: +27 82 415 8253
Email: dechivers@deloitte.co.za

Daniella Kafouris
Associate Director: Risk Advisory Africa
Mobile: +27 72 559 0360
Email: dkafouris@deloitte.co.za