Comply proactively with PoPI, says the PBT Group

The industry remains abuzz with talk about the recently Gazetted Protection of Personal Information (PoPI) Act, yet the compliance rate of South Africa's enterprises varies significantly. For Small Medium Enterprises (SMEs) the pace to become compliant is considerably slower, according to the opinion of information management company, the PBT Group.

Image: www.freedigitalphotos.net

The South African Government is following in the footsteps of its international leaders regarding privacy legislation; however PoPI is not merely following a fashion fad, but rather is a legislation that needs to be complied with for very good reasons.

Yolanda Smit, Strategic BI Manager of the PBT Group, said: "The reality is that cybercrime, with identity theft in particular, is booming globally and South Africa has also been impacted on. It is for this reason that PoPI, amongst other legislation, is being implemented in an effort by the South African Government to fight cybercrime, increase public awareness of the risk here, and ensure that personal information is protected."

The PBT Group is of the opinion that PoPI is definitely a valuable addition to South Africa's legislation, yet the value will be very dependent on the effective implementation and regulation of this Act. Continued Smit: "The unique economic conditions in South Africa, which incorporate a number of global enterprises as well as an even larger mix of smaller enterprises, sole proprietors and informal enterprises, mean that the Regulator really does have his job cut out for him."

"The ultimate goal of the Act is to establish a balance between everyone's right to privacy and everyone's right of access to information. The downside, however, is that the Act seems ambiguous and difficult to interpret at this stage - which can be the reason for the slow uptake."

While clarity is expected as soon as the Regulator is effectively up and running, the PBT Group believes that the time is now for businesses of all sizes that deal with data, at least to start the journey towards interpreting the Act and coming to grips with its potential impact on operations - as compliance will inevitably become a legal requirement in the near future.

Understanding PoPi

The volume of data that a business is dealing with actually has little impact on the effort required to comply. Effort and cost of compliance is rather the sum product of the diversity of the types of data subjects (customers, employees, shareholders, vendors etc.); disparity of the systems processing personal information; complexity and fragmentation of security controls, as well as exposure to third-party operators that process information on behalf of the organisation.

"The first critical success factor is accepting the fact that PoPI is not an IT Act. There is no single standalone IT system that will be the silver bullet to ensure compliance. In fact, protecting personal information is an enterprise issue prevalent in all dimensions of a business (process, people, and systems). It should also be noted that PoPI is a continuous compliance legislation - complying is not a one-off exercise that, once all the check-boxes have been ticked, a compliance status is achieved and filed," continued Smit. "One's compliance status is only as strong as the last incident that occurred (whether proven or alleged)."

The very first step or action that businesses should take is to appoint an Information Officer, if one is not already in place. The Information Officer was first required with the commencement of the Promotion of Access to Information Act (PAIA), some years ago; however, by default this responsibility rests on the shoulders of the CEO unless otherwise delegated. In some organisations, this role is being fulfilled by the Data Governance or Governance Officer. By appointing a person in this role, and clearly defining his role and responsibility, compliance to two Acts can be ensured.

Together with the Information Officer, businesses should also implement a breach management capability.

"It is important to note that no control will be failsafe. Organisations dealing with data will know that cybercriminals learn fast and continuously, and, therefore, it is just as important to have a robust breach management capability as it is to have a breach prevention capability. The risk to one's reputation can be mitigated significantly if incidents that do occur are dealt with swiftly and effectively."

Once the governance and management structure is in place, a concerted effort should then be taken to assess the organisation and identify areas that are at risk of non-compliance. This should follow a traditional top-down assessment approach to ensure that effort is prioritised and focused on areas of highest risk.

Concluded Smit: "It is important for businesses to remember that accountability of PoPI rests with top-level business management and, therefore, all effort to comply should be a concerted joint partnership within the business - one that incorporates its IT department, but does not depend solely on IT. Businesses can partner information management experts in the field who understand the Act and can offer clients various services to assist with compliance. Complying with PoPI will eliminate real risk with severe repercussions for an organisation. By addressing it proactively (and not procrastinating until the Act fully commences) businesses will have a leading advantage and this could actually be turned into a competitive edge by instilling trust with stakeholders."