Preparing for PoPI - a checklist

The Protection of Personal Information Act (PoPI) may not have been made effective yet, but businesses need to make compliance one of their top priorities for 2017. This is according to Wayne Clarke, managing director of Metrofile Records Management, who states that the appointment of the Information Regulator by the President is imminent.

©Maksim Kabakou via 123RF

“From the appointment of the regulator, companies will officially have one year to update their databases and practices or risk facing massive fines, or even imprisonment for liable individuals. While many businesses have already proudly proclaimed that they are PoPI compliant, there is a startling number of companies that are not,” he says.

“We see quite a few companies that are either behind schedule on their PoPI compliance plans, or that have not started a meaningful compliance strategy at all. In fact, the 2015 *Records and Information Management Trends Index* commissioned by Metrofile, indicated that 22% of South African companies have not started to implement compliance measures related to their record storage and management.”

Clarke notes that South African businesses should realistically already have started their PoPI implementation processes, in order to ensure compliance by the cut-off date. “Converting any company’s records and information systems to reach a state of compliance, is a long and expensive process, which is why organisations realistically require a multi-year time frame. That said, it is not impossible for a company to reach a state of compliance within 12 months.”

The first step, according to Clarke, is to outsource the company's conversion strategy. "In light of the significant pressure that is now on unprepared businesses, the decision to outsource their PoPI related responsibilities such as secure record storage, management and destruction, may be an ideal solution – especially considering the enormous penalties and reputational damage that could result from a violation. Keep in mind however, that accountability cannot be outsourced to an information management provider. A company is still responsible for ensuring and enforcing its own compliance.

Clarke provides the following PoPI checklist to further assist businesses:

Month 1: Find a service provider fast

Now is the time to find a PoPI compliance service provider. Reputable law firms are often considered the best options for lead service providers in this instance, but specialist record storage, software and training service providers are also viable options, depending on the nature and needs of the business.

Month 2: Classify and understand

The first step in the company's PoPI compliance plan, is to start classifying the information that is kept on file. Know exactly which of the company's data contains personal information, determine why it is being retained, and define how long it needs to be kept. If the information in question is not essential to the company's operations, earmark it for deletion.

Month 3: Conduct an internal audit

Your company's contract with the chosen service provider should be in the final processes of being negotiated. Utilise the first weeks of October to conduct an initial internal audit of the company's processes used to collect, record, store, disseminate and destroy personal information.

Use the information gathered in this audit to make an initial assessment of where information is at risk or is being duplicated.

Month 4: Deal with unnecessary information

The first of PoPI's compliance conditions, is the purpose requirement. The service provider's first task should be to assist in destroying all pieces of personal information that the company does not need. Both digital and physical files need to be processed by a reputable document destruction service, in order to guarantee that no information is compromised.

Month 5: Transparency is key

A company must notify its data subjects, where, how and why their data is being stored. With this in mind, the company now needs to start work on a process to inform clients the name and address of the company processing their information, whether said information is voluntary or mandatory, and what this information will and will not be used for.

At the same time, the service provider should already be in the process of updating and securing the company's information and data backup system. This is no quick process, and a company needs to be prepared to work around any interruptions that might be caused by this over the coming months.

Month 6: Evaluate data capturing processes

The compliance condition for this month is information quality. With the service provider still updating data storage, this month should be spent in consultation with them on how to maintain data value, and devising reasonable processes for employees to follow in order to effectively capture and file accurate information.

Month 7: Staff training

While in the process of changing employee procedures, this month is also the time to address the compliance condition of responsibility.

All company employees are responsible for conforming to the regulations regarding clients', employees and company personal information. Therefore, the company-wide policies, responsibilities and roles for data handling, have to be established and complied with.

Month 8: Focus of secondary data processing

For the compliance condition of additional processing, the service provider and the company this month need to lay down clear-cut processes for the further processing of existing information.

Conducting client updates and sharing information between departments must be in line with the same regulations that apply to initial data collection. Keep in mind that the company also requires a procedure to deal with data subject objections and requests.

Month 9: Information security

The PoPI legislation requires all-round security as part of its compliance conditions. This should be the service provider's forte, meaning that now is the time to officially gain clarity from the service provider on the following functions, going forward:

- How personal information will be protected from unauthorised or unlawful access, unnecessary mutilation or deletion.
- How to ensure the reliability of personal information, both from a technical and operational standpoint.
- How these standards will be ensured with all parties that receive data from, or process data on behalf of your company.

Month 10: Define boundaries

The penultimate compliance condition to address is the restriction of processing. A defined boundary needs to be established regarding the processing of personal information. Keep in mind that a company cannot claim ownership of any personal information, and the company now needs to relay clear instructions to its employees on what they can and cannot do with said information.

Discuss the framework whereby clients and employees will provide consent and be furnished with a clear and understandable indication of how their information is used.

Month 11: Time to troubleshoot

If all is going to plan, the majority of the company's PoPI compliance procedures are in place and ready to be utilised. Keeping in mind that the company should be ready to engage the regulator and the public from next month, the service provider now needs to assist in systems checks and final troubleshooting of the existing procedures and systems.

Month 12: Client and stakeholder involvement

Data subject involvement is the final compliance condition to master. With the majority of the company's PoPI conditions in order, the company should be ready to withstand the intense scrutiny of its existing and potential clients.

If you have not done so already, inform your clients of their right to update or delete personal information from any of the company's systems. Remind the client that they may, at any time, request a validation from the company as to whether their personal information is held. They are also entitled to a description and reason for the retention of said personal information.

Deadline month: Engage the Regulator

The Information Regulator's powers are in full effect at the end of this month, and so are the penalties for non-compliance. By now, your company needs to be in a position to declare the processing of personal information to the Regulator.

The company now needs to look towards maintaining its levels of compliance. Under the new regulator, companies need to commit to annual reassessments of their information systems. The regulator will also continuously be looking at new types of personal information, and businesses will need to stay abreast of these changes as they happen.

"It is important for businesses to understand that they can achieve most if not all of the requirements set out in the PoPI Act. There are of course more and less vital aspects of PoPI, and companies reporting honestly to the new Information Regulator, are likely to be given additional time to attain compliance with some of PoPI's less pressing points. This grace will of course be reliant on the level of compliance that the company has already attained," Clarke concludes.

For more, visit: https://www.bizcommunity.com