Institute of Directors in Southern Africa

QUICK GUIDE TO PoPI FOR DIRECTORS

Introduction

The Protection of Personal Information Act (PoPI) aims to bring South Africa’s privacy laws in line with international norms and to give substance to the Constitution’s protection of privacy. It’s based on the European data-protection directive and aims to protect sensitive private information and sets guidelines for how companies handle it.

PoPI was signed into law late in 2013 but there has been no date for its commencement as yet. Some legal experts expect this to occur in March 2014, but thereafter the regulations made under the Act may still need to be finalised.

There could be quite a delay between the Act coming into force and the publication of the regulations. During this period, companies will have to rely solely on the Act for guidance. However, the Act allows companies a year in which to comply.

Areas of focus

Data collection

What

- PoPI covers information relating to clients, suppliers, employees, persons receiving marketing information, persons present on premises etc. Personal information which is protected by the Act includes all of the following: race, gender, sex, marital status, sexual orientation, age, physical and mental health, religion and criminal and financial records.
- Sources of information types that are impacted upon include payroll data, CVs, employment applications, security records, standard HR information (such as evaluations and reviews) and even internal e-mails.
- At the same time, the existing manuals created in terms of the Promotion of Access to Information Act (PAIA), which spell out the company’s policy in terms of providing access to the information it holds, must be updated in line with PoPI.

How

- Explicit permission needs to be given for collection and use before data is collected.
- Data can only be collected from public domain; no more rental database lists, and no “inside info” lists.

Why

- Companies will also need to motivate why they need to keep certain data.
- Individuals need to be informed for how long information will be kept.
Data use and storage

- PoPI has significant implications for marketers because mobile numbers and e-mail and postal addresses fall under the category of personal information.
- Currently, marketers may use mobile numbers or e-mail addresses for unsolicited marketing material (or spam) provided that recipients can easily opt out. Once PoPI comes into effect, this will no longer be possible. Marketing material will only be able to be sent to individuals once their consent has been obtained, the so-called opt-in model.
- Companies must do the minimum with collected information, and always in line with the original reason for collecting it.
- In these days of cloud computing, it’s worth noting that PoPI does not allow sensitive private information to be stored in foreign jurisdictions that have inadequate data-protection regulations. It’s thus important that directors investigate where the servers of third-party providers of digital storage are located.
- The data must be secure. Companies must protect against unauthorised access, accidental destruction, theft and information leaks.
- Data subjects can request disclosure about whether an organisation holds their private information, and what information is held. They may also request the correction or deletion of information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- Those with access to data must sign non-disclosure agreements or similar documents.

Data sharing

- To discharge their obligations under PoPI, companies must keep the types of information specified by the Act physically secure, and restrict access to it in line with the Act.
- Personal information may not be sold or shared unless permission given by the data subject.
- Such information should be destroyed once the reason it was collected is no longer valid.

Implications for Directors

There are many reasons why POPI deserves board level attention, among them the following:

- **Top-level responsibility.** Under PoPI, chief executives are automatically information officers, who must ensure compliance with PoPI, unless they delegate the job. However, because of the complexity of complying with PoPI, they should take care to keep themselves informed of what the company is doing even if they do delegate.

- **Effect on due diligence.** Furthermore, directors may not be fully aware of the complexities relating to board compliance with PoPI. In particular, directors need to be cognisant of the need to see PoPI within the context of the broader regulatory framework, especially as POPI often allows for exceptions to a requirement based on the requirements of another law. The duty contained in the Companies Act to avoid appointing directors who have committed certain offences may, in certain instances, override PoPI’s requirement that criminal records may not generally be requested or held.

Another example of the ongoing importance of monitoring PoPI may be especially relevant to small, medium and micro enterprises (SMMEs). While PAIA manuals must comply with PoPI, it needs to be borne in mind that certain types of SMME are exempted from the need to have PAIA manuals at all. This exemption might well be updated with one that covers the PoPI aspects of the PAIA manual.

Assistance for IoDSA Members

PoPI creates many areas of legal uncertainty, so compliance is not something that can be swiftly and definitively achieved. Directors need to understand the issues and stay on top of them, as well as any changes to the PAIA regulations.

Members of the IoDSA are automatically updated via the IoDSA’s Direct Law service, and a POPI compliance risk management plan should be released on [www.crm.co.za](http://www.crm.co.za) by April 2014.