POPI CHECKLIST:

Take the Guesswork out of Complying

www.contadorinc.co.za
info@contadorinc.co.za
087 287 7436

8 CONDITIONS TO COMPLY WITH

The new Protection of Personal Information Act, POPI for short, stipulates how businesses should collect, process, share, store, and use the personal information that they have gathered from customers, suppliers, employees, and any other stakeholders.

Here are the 8 conditions with which you must comply:

- [ ] **Accountability:**
  You should make sure that you process personal information gathered in a lawful way and in accordance with the conditions and requirements stipulated in the act.
- [ ] **Processing limitation:**
  You should process personal information only for reasons permitted by law, and in a way that does not infringe on their privacy.
- [ ] **Purpose specification:**
  You should gather and keep personal information only for a specific purpose.
- [ ] **Further processing limitation:**
  If you want to process personal information further, it should be compatible with the original purpose of collecting the information.
- [ ] **Information quality:**
  You should make sure that the personal information collected is complete and accurate.
- [ ] **Openness:**
  You should inform individuals that you collect their information, as well as the reason why you collect it and how you will use it.
- [ ] **Security safeguards:**
  You should take reasonable steps to keep the information gathered secure.
- [ ] **Data subject participation:**
  Should someone request access to their personal information that you hold, or request that you correct or delete the information, you should comply.

POPI ACT IMPLEMENTATION CHECKLIST

Any individual or legal entity needs to comply with the POPI Act when handling personal information of a 'data subject'. A data subject is defined as the individual or entity whose information is being processed, and this includes your customers, prospective customers and people you market to, employees, suppliers, investors, etc.

These are the simplified POPI implementation requirements:

Gap Analysis and Preparation

- [ ] Audit the processes used to collect, record, store, process, and destroy personal information and identify gaps where you do not comply with POPI and identify any security risks. This includes the steps taken to collect, store, view, change, transfer to other systems, back-up, clean, and destroy information.
- [ ] Specify those third parties with which personal information is shared, like outsourced partners, managing agents, auditors, bookkeepers, lawyers, etc.
- [ ] Large companies should notify the information regulator of any personal information processing activities.
- [ ] Small companies don't need to notify the regulator, only if something goes wrong, like if your laptop or the hard drive that contains personal information is stolen.

Training and Responsibilities

- [ ] Make sure that anybody that can be held accountable is aware of the penalties should they not comply with the Act.
- [ ] Provide training to all staff members that handle personal information. Ongoing training is needed, especially when new processes, services, or products are added.
- [ ] Provide comprehensive training for the Information Officer.

POPI ACT IMPLEMENTATION CHECKLIST

Policies and Documentation

- [ ] Make sure that your company website and documentation is compliant with the Act.
- [ ] Make sure you have published policies in place to guide employees on their responsibilities.
- [ ] Make sure that you have appropriate agreements in place that stipulate what third parties can and can't do with the personal information that you share with them.
- [ ] Review your websites and include the necessary information, like a privacy policy and cookie notifications.
- [ ] Update or create your PAIA manual in accordance with the Promotion of Access to Information Act (PAIA).

Collecting Personal Information

- [ ] Define the reasons why you gather personal information and how it is processed.
- [ ] Define how you collect information about your customers, staff, suppliers, or other partners. For example: telephonically, through a website, application form, or email.
- [ ] Define how you ensure that the information that you have gathered is complete, accurate and up-to-date.
- [ ] Inform data subjects that you collect their data and why. Make sure that they explicitly give you permission to collect their information.
- [ ] If you have received personal information from third parties, you need to confirm that the data subject is aware of this.

POPI ACT IMPLEMENTATION CHECKLIST

Processing Personal Information

- [ ] Limit processing to ensure that the way you handle information is lawful and reasonable.
- [ ] Only process information for the reason that it was collected, and no other. If you want to process it for another reason, you need to get permission from the data subject first.
- [ ] Notify employees that their personal information is captured, retained, and processed, and the reasons why and how their information will be used.

Sharing Personal Information

- [ ] A data subject has the right to know whether any third parties have access to their information and who these parties are.
- [ ] Inform your data subjects if you share their personal information with a third party and why.
- [ ] Notify employees if their information is being shared with third parties, like accountants, payroll, SARS, and the Department of Labour.

Storing Personal Information

- [ ] Define who is accountable for the safeguarding of documents and data.
- [ ] Take steps to prevent the information from being lost, damaged, or unlawfully accessed.
- [ ] Monitor ongoing data protection and look out for threats and opportunities.
- [ ] Determine whether the software packages that you use are secure and passwords are changed frequently.
- [ ] Keep your information up-to-date and correct.

POPI ACT IMPLEMENTATION CHECKLIST

Destroying Personal Information

- [ ] Define the process for destroying personal data. Make sure you know where everything is stored, like hard copies, soft copies, images, video, voice recordings, CCTV, biometric, and archives.
- [ ] Delete all personal information that is no longer needed.
- [ ] Should a data subject instruct you to destroy their data, you need to comply.

Other

- [ ] Anybody has the right to know what information you hold and whether third parties have access to it. If someone requests to see their information that you you hold, you need to comply, free of charge.

Please note that this list is not exhaustive. Every business has different needs and requirements.

POPI was signed into law in November 2013, but the commencement date has not yet been finalised . The Act will only come into effect once this date is announced, after which companies will have to comply within 12 months.

If you need clarification on any of the above points, or you would like to get our help with implementing POPI requirements in your business, get in touch with us.

www.contadorinc.co.za | info@contadorinc.co.za | 087 287 7436