instacom
ONE COMPANY - INFINITE SOLUTIONS

Are You POPIA Compliant?

If you answer NO to five or more of these questions or are unsure of any of them, chances are you are not POPIA Compliant!

		✓	✗	?
1	Do you process special personal information such as religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal records, CCTV Footage, contact details etc.?			
2	Do you obtain consent from data subjects to process personal Information?			
3	Do you store personal information with a third party?			
4	Is the devices on which data is stored secure?			
5	Is the platforms on which data is stored secure?			
6	Do you have a data breach notification policy and incident response plan in place?			
7	Do you provide the personal Information to any third parties?			
8	Do you provide personal information to third parties in “good faith” (no agreements)?			
9	Do you have confidentiality/privacy agreements in place separate from your employment contract or service level agreements?			
10	Did you receive POPI Act awareness training / schedule training for your company?			
11	Do you have a registered information officer appointed? How do you destroy Personal Information after retention periods?			
12	Do you have “best practice” solutions?			
13	Do you have a PAIA Manual submitted at the Human Rights Commission?			

DID YOU KNOW?

Instacom believes in doing the right things right.
Respect is a core value at Instacom. When you do business with us, you can expect confidentiality and privacy agreements as part of our contract with you, because we take the protection of your data seriously.
That is respect.

Instacom’s hardware and software solutions are fully POPIA Compliant. We capture and store data securely. Even if you have the relevant permissions, data will be displayed in a secure, compliant way.

DID YOU KNOW?

The most important points to consider when processing personal information:

Record your data and personal information.

Know where, what type of and by whom all personal information is being processed (information storing, controlling and deploying).

Evaluate all service agreements relating to data processing.

Update contracts accordingly and keep them proximate – clear roles should be defined for everyone in the processing chain.

Prepare for dealing with numerous regulators & authorities.

The Information Regulator, SARS and Financial Services Board, etc.

Prepare to execute an all-inclusive POPI assessment by seeking practical legal advice & guidance.

Rather consult with professionals & spend adequate time and money to ensure you are POPI compliant.

POPI and your business: In a nutshell

Section 7 of the POPI Act relates to security safeguards. It requires businesses to secure the integrity and confidentiality of personal information by applying security practices and procedures that protect the business against information threats and vulnerabilities.

Section 19 of the POPI Act is aimed at preventing the loss, damage or unauthorised destruction of personal information by identifying the personal information risks to which the business is exposed to and how these risks are mitigated and managed.

Businesses should consider whether their current measures will leave the personal information in their possession or control vulnerable to loss, damage and unauthorised access.

Businesses should therefore take reasonable steps appropriate to the type of information being processed, the size of the business as well as the cost and time relating to the implementation of these measures.

Section 19 of the POPI Act goes further to explain that the reasonably foreseeable internal and external risks are identified by an external audit to implement Information Security management systems, standards or frameworks.

- This will establish where the vulnerabilities in the business lie, and which safeguards to implement. These safeguards can range from technical solutions, such as firewalls, anti-virus and encryption, etc., to practical implementation of policies and procedures for processing information and preventing data breaches. In the global economy it is becoming increasingly important to focus on cyber security, which should also be included in these policies and procedures.

- This section also requires businesses to verify whether these measures are effective and updated on a regular basis.