ATG DIGITAL
Driving Change

WHAT IS THE POPI ACT AND HOW DOES IT AFFECT ME?

"POPI applies to every person and business within South Africa"

THE ONLY EXEMPTIONS:

Household/Personal activities; Sufficiently de-identified information; Some state functions including criminal prosecutions and national security; journalism under a code of ethics

ABOUT POPI

“POPIA is a piece of legislation designed to protect the personal information of both individuals and businesses which is processed by both private and public bodies.”

POPIA is important because it protects data subjects from harm like theft and discrimination, and protects the collectors of information by providing guidelines within which to operate.
POPIA does not stop you from processing information and doesn’t always require you to get consent from data subjects, but it does impose a framework within which to operate and a set of rules to ensure the security of the information processed.

Compliance requires a serious shift away from thoughtless, excessive and random collection of personal information as well as the sharing of information (whether intentional or not) to unauthorised third parties.
We should be concerned not only with the legalities of information security but also with taking the utmost care of our staff, customers, suppliers and other information sources in order to uphold their rights.

IMPLICATIONS OF NON-COMPLIANCE

Compliance with POPIA is the responsibility of every organization within SA. Now that the compliance notice period is over, the risks of non-compliance are severe, with POPIA having serious punishments for offenders.

Depending on the seriousness of the breach, punishments could include:

- Administrative fines of up to R 10 million or 10% annual turnover
- Up to 10 years imprisonment for the CEO
- Damages rewarded to the Data Subjects
- Notifying every potentially affected Data Subject

For small offences, fines would be lower, or you'd receive a warning and be flagged for supervision. Although even this would not be a desirable outcome, as enormouse time, effort and money will be spent, to mitigate the risks of being in the Regulators' and publics' bad books.

DEFINITIONS

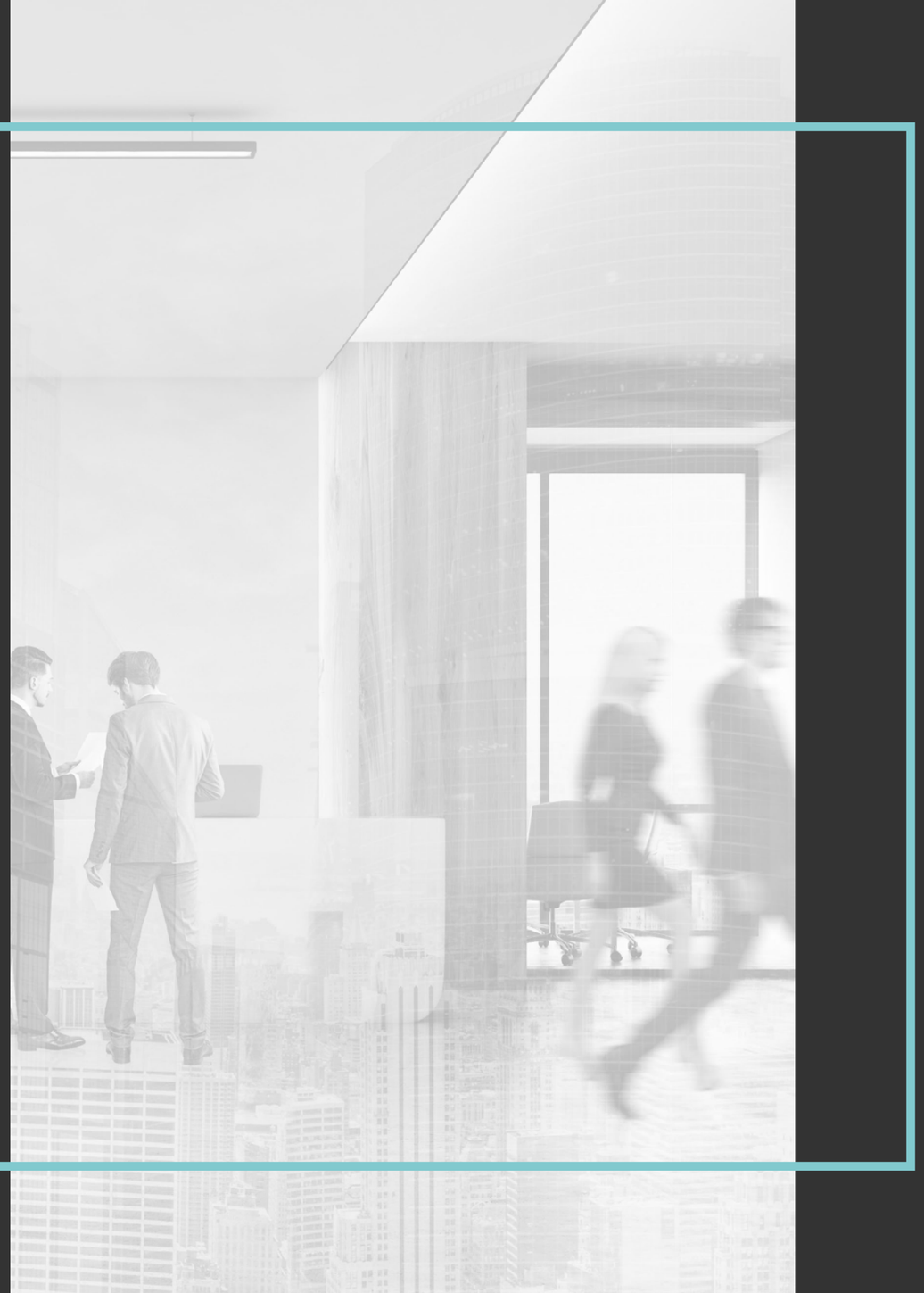
DATA SUBJECT
An identifiable natural person or existing juristic person.

PERSONAL INFORMATION
Relating to the Data Subject, including but not limited to: race; marital status; national/ethnic/social origin; sexual orientation; age; health; religion; culture; education; financial/medical records; contact/location information; biometrics; name.

PROCESS
Any means of collecting, disseminating, analysing, storing or detroying information.

RESPONSIBLE PARTY
The business who decides on the reasons, type, and methods of collection, responsible for ensuring that they, as well as their operators, are compliant with the conditions required for lawful processing.

OPERATOR
A person or business who processes information on behalf of the Responsible Party.



Aside from the above consequences, and even without formal enactment, being non-compliant and risking breach would:

- Indicate you don’t care about privacy, leading to poor customer relationships and low levels of trust from both customers and general public

- Cause reputational damage, and with the power of social media in the 21st Century, this could be catastrophic. Unfortunately, the saying “There is no such thing as bad publicity” no longer applies, especially when there is legislation being contravened and public forums where possible breaches can be shared and discussed

POPIA COMPLIANCE CHECKLIST

The road to compliance is long and sometimes arduous, but it is not necessarily complicated. That said, every business is unique, and elements of processing may exist which require special care and attention. For that reason, it is recommended that you retain the services of appropriate legal advisors to ensure your processes are complete. The following list is a mere summary of what needs to be done and is by no means exhaustive.

1. Appoint an Information Officer who will take responsibility for the compliance process.
2. Audit all the information you use, as well the systems used to process it.
3. Define the purpose of the information gathering and processing: it must be collected for a specific, explicitly defined and lawful purpose related to a function of your organization.
4. Ensure information quality: make sure the information is complete, accurate, up to date and not misleading.
5. Check the retention periods to ensure you're not keeping information for longer than necessary.
6. Decide how you will ensure its safety by changing physical or IT systems to ensure the integrity of the information.
7. Notify the Data Subject whose information is being processed, as they have the right to know this is being done and why. They must be told the name and address of the company processing their information, as well as whether the provision of the information is voluntary or mandatory. If voluntary, give them the option to request that their information is deleted or de-identified.
8. Notify the Information Protection Regulator (once established) about your actions: the categories and purpose of processing personal information.

TO ENSURE YOUR COMPLIANCE, YOU NEED TO DO THE FOLLOWING:

- Read and sign the POPIA policies and documents that we, ATG Digital, provide.
- Place the POPIA notices at your entry points
- Safeguard your user login details.
- Ensure that access to the backend is only granted to essential staff
- Ensure that staff understand their obligations under POPIA and that they have been properly screened for trustworthiness
- Initiate device security protocols to ensure that staff never leave their computers/phones unlocked and unattended
- Initiate physical and IT security protocols to ensure the safety of computers, servers and networks
- Take care not to print reports from the backend without adequately de-identifying the data
- Do not share data with any third party or engage in any futher unauthorised processing
- Do not store information for longer than is necessitated by purpose

WHAT ARE YOUR COMPLIANCE OBLIGATIONS WHEN IT COMES TO ATG'S DEVICES

Under POPIA, ATG and the relevant security company are collectively considered as "The Operator". As the end-user of the ATG devices, you are defined as "The Responsible Party".

When our devices are used, the information is encrypted and instantly uploaded to a cloudbased platform. No data is stored on the device. This means that if the device is lost, stolen or tampered with, NO ONE will be able to access the information that has been captured.

Information is stored on Google Cloud Services, a platform selected for its worldrenowned security systems and compliance with international privacy legislation.

The information on the cloud can only be accessed via the customer back-end by:

- Authorised personnel of the Responsible Party for their purposes
- Authorised personnel of ATG at the request of the Responsible Party, an officer of the law, or the Data Subject

To ensure the safety of all the data that we gather on behalf of responsible parties:

- Passwords are required by both the Responsible Party, as well as by all duly authorised ATG personnel.
- All staff are carefully screened before employment and sign an NDA as part of their employment contract.

CARE TO COMPLY?

Disclaimer: The information in these booklets is for information purposes only and is distributed as a courtesy to our clients and prospective clients. It is by no means legal advice and your own POPI compliance process should take place with the supervision of adequately trained and objective professionals.

ATG DIGITAL

Driving Change

010 500 8611

support@atthegate.biz

www.atgdigital.biz