How does POPI apply to our business?

POPI generally applies to all processing of Personal Information that is stored in our records. POPI therefore applies to all our processes for our clients (and related parties), employees and suppliers.

What do you need to do to start your POPI Compliance journey?

You need to attend all training that will be provided and ensure that you have read the Lawtons Data Privacy Policy and Procedures, prior to the commencement of the Act on 1 July 2020.

Our POPI Steering Committee consists of:

Jeff Buckland (Chairman of the MB, Director, POPIA Information Officer)
Veronica Vurgarellis (Member of the MB, Director, POPIA Deputy Information Officer)
Dimitra Kouvelakis (General Counsel)
Lindi Mengezeleli (Head of HR)
Shaz Randle (Finance Manager)
Winnie Masilela (Marketing and Business Development Manager)
May-Elaine Thomson (Head of Projects & Operations)
Leon Mat-Hope (Risk & Compliance Manager)
Juanita Rangate (Payroll & HR Consultant)
Chris Browne (Head of IT)

Data Protection Procedure

1. Introduction

These processes and procedures ("**Procedures**") aim to promote compliance with Data Privacy Legislation and principles within Lawtons.

This Procedure must be read together with the Lawtons Data Privacy Policy. It is aimed at providing clear and concise procedures and processes for directors and employees to adopt to ensure compliance. This Procedure shall be binding on all directors and employees.

1.1. Processing Limitation

Data Protection Legislation restricts the way we may Process Personal Information for our clients, employees and service providers (referred to hereinafter as the "Data Subject"). Processing must be adequate, relevant and not excessive given the purpose for which the Personal Information is Processed. These restrictions are not intended to prevent Processing, but to ensure that employees Process Personal Information lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject.

Data Protection Legislation allows Processing under specific circumstances, subject to consent for obtaining and requiring the information from the Data Subject (relevant clauses have been included in the client engagement letters, briefs to counsel, etc.).

Employees may only collect Personal Information that is required for their job duties, or as may be required by law, and may not collect excessive data. Employees must also ensure any Personal Information Processed is adequate and relevant for the intended purposes.

Employees must ensure that when Personal Information is no longer needed for specified purposes, it is deleted or processed in accordance with Lawtons' data retention procedures (described in more detail below).

A Data Subject must consent to the Processing of their Personal Information.

Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if the intent is to Process

Personal Information for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Employees need to file electronically on iManage the consent captured and keep records of all consents (both given and withdrawn by a Data Subject) so that Lawtons can demonstrate compliance with consent requirements.

1.2. Purpose Specification and Further Processing Limitation

Employees may only collect, store, update, destroy, or otherwise Process Personal Information for specified purposes. Personal Information must not be further Processed in any manner incompatible with those purposes.

Employees will need to ensure that the Data Subject is aware of the purpose for which Lawtons is collecting information. It is essential that the letter of engagement are completed with the Data Subject when the matter is initiated as the letter of engagement has been revised to include the POPIA requirements.

Employees cannot use Personal Information for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject is informed of the new purposes and they have consented where necessary.

1.3. Information Quality

Personal Information must be complete, accurate and not misleading, and kept up to date. It must be corrected or deleted without delay when inaccurate.

Employees must ensure that the Personal Information we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Accuracy of any Personal Information must be verified at the point of collection and at regular intervals afterwards. Employees must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Information.

1.4. Openness

Employees must take reasonably practicable steps to ensure the Data Subject is aware of various matters related to the collection of Personal Information, including, but not limited to:

- the type of Personal Information collected and the source from which it is collected;
- the purpose for which Personal Information is collected and the particular law authorising or requiring the collection of Personal Information (for example FICA requirements);
- whether or not the supply of Personal Information is voluntary or mandatory;
- consequences of failure to provide required Personal Information;
- whether Lawtons intends to transfer the information to another country and the level of protection afforded to that information in that country;
- the recipients of the information, e.g. Docfox, and Amazon Web Services located in the Republic of Ireland (where all Personal Information is stored);
- the Data Subject's right to access, rectify, or object to the collection or Processing of the information; and the right to lodge a complaint with the Information Regulator.

Whenever Lawtons collects Personal Information directly from Data Subjects, including for human resources or employment purposes, Lawtons must provide the Data Subject with all the aforementioned information. This information must be presented when the Data Subject first provides the Personal Information.

When Personal Information is collected indirectly (for example, from a third party or publicly available source), Lawtons must provide the Data Subject with all the above information as soon as reasonably possible after collecting or receiving the Personal Information. Lawtons must also check that the Personal Information was collected by the third party in accordance with applicable Data Protection Legislation and on a basis which contemplates Lawtons' proposed Processing of that Personal Information.

Security Safeguards

1.5. Protecting Personal Information

Personal Information must be secured by appropriate and reasonable technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

Lawtons will endeavour to identify all reasonably foreseeable internal and external risks to Personal Information in Lawtons' possession or under its control. In this regard, it is important that employees are responsible for protecting the Personal Information that is Processed by Lawtons (to the extent that employees are involved in the Processing of this Personal Information). Employees must adhere to the security measures imposed by Lawtons against unlawful or unauthorised Processing of Personal Information and against the accidental loss of, or damage to, Personal Information. Employees must exercise particular care in protecting Special Personal Information from loss and unauthorised access, use or disclosure.

Employees must follow all procedures and technologies Lawtons puts in place to maintain the security of all Personal Information from the point of collection to the point of destruction. Employees may only transfer Personal Information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Employees must maintain data security by protecting the confidentiality and integrity of the Personal Information, bearing in mind that:

1.5.1.1. confidentiality means that only people who have a need to know and are authorised to use the Personal Information can access it; and

1.5.1.2. integrity means that Personal Information is protected against loss, damage or unauthorised destruction.

Employees must comply with, and not attempt to circumvent, the administrative, operational, physical and technical safeguards and standards that Lawtons implements and maintain to protect Personal Information.

Anyone who Processes Personal Information on behalf Lawtons is required to Process Personal Information only with the knowledge or authorisation of Lawtons, and to treat Personal Information which comes to their knowledge as confidential.

Employees are to adopt a clean desk policy to ensure that no personal information or confidential information is left lying on their desks at any time.

Employees are not permitted to copy any information onto external devices such as external hard drives or USBs without the consent of the Data Subject.

Employees are not permitted to connect to any insecure hotspots.

1.6. Reporting a Personal Information Breach

Employees must immediately report any breaches to their director, head of HR or the Information Officer or Deputy Information Officer.

1.7. Data Subject Participation

Data Subjects have rights when it comes to how Lawtons handles their Personal Information. These include, depending on the Data Subject's location, the right to:

- be notified that Personal Information is being collected;
- be notified of a Personal Information breach;
- access to the Data Subject’s Personal Information held by Lawtons;
- request the correction, destruction or deletion of Personal Information;
- restrict our Processing of the Data Subject's Personal Information;
- object to direct marketing;
- request that Lawtons transfer their Personal Information to a third party in an easily accessible format;
- object to automated decision making; and
- submit a complaint to the Information Regulator.

1.8. Responding to requests to access Personal Information

Data Subjects have the right to request access to their Personal Information Processed by Lawtons. Employees must immediately forward any Data Subject request received to their director and comply with the below. When a Data Subject makes an access request (each an "**Access Request**") Lawtons shall take the following steps:

- log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
- confirm the identity of the Data Subject who is the subject of the Personal Information. For example, we may request additional information from the Data Subject to confirm their identity;
- search the Lawtons databases, systems, applications (Elite & iManage) and other places where the Personal Information which is the subject of the request may be held; and
- confirm to the Data Subject whether or not Personal Information of the Data Subject making the access request is being Processed.

2. RECORD RETENTION

2.1. There are legal and regulatory requirements for Lawtons to retain certain Records and Personal Information, usually for a specified amount of time. Lawtons also retains Records and Personal Information to help the business operate and to have information available when needed. However, Lawtons does not need to retain all Records and Personal Information indefinitely, and retaining Records and Personal Information can expose Lawtons to risk as well as be a cost to the business.

2.2. This section pertains to all Records of Personal Information that Lawtons holds or has control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It also covers records of Personal Information that are held by third parties on Lawtons' behalf, for example cloud storage providers or offsite records storage. It also covers Records of Personal Information that belongs to Lawtons but is held by employees on personal devices. Together the above shall collectively be referred to as "**Records**".

2.3. Lawtons shall comply with the following in respect of Records retention:

COMPANIES ACT 71 OF 2008	
24. Form and standards for company records 1. Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of this Act or any other public regulation must be kept- a) in written form, or other form or manner that allows that information to be converted into written form within a reasonable time; and b) for a period of **seven years**, or any longer period of time specified in any other applicable public regulation, subject to subsection (2).	**7 years**

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013	
14. Retention and restriction of records 1. Subject to subsections (2) and (3), records of personal information must **not be retained any longer than is necessary** for achieving the purpose for which the information was collected or subsequently processed, unless— a) retention of the record is required or authorised by law; b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities; c) retention of the record is required by a contract between the parties thereto; or d) the data subject or a competent person where the data subject is a child has consented to the retention of the record. 2. Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes. 3. A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must— a) retain the record for such period as may be required or prescribed by law or a code of conduct; or b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record. 4. A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).	**Not longer than necessary**

2.4. Roles and Responsibilities

Responsibility of all Employees

All Employees must comply with all Records retention procedures, any communications suspending Records disposal and any specific instructions given by Lawtons management or the Information Officer or Deputy Information Officer as appointed by Lawtons from time to time. Failure to do so may subject Lawtons, its employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with any Records retention procedures may result in disciplinary sanctions, including suspension or termination of employment.

Further information:

Privacy/Disclaimer Website/emails	***COVID-19:*** *Lawtons Africa has all necessary public health protocols in place throughout our premises. All visitors, clients and staff must wear masks at all times and will be temperature-scanned on arrival. We are able to offer a seamless service remotely and are available to you via email or mobile when working off-site. Please contact me directly on +27 73 556 1131.* *Our meeting rooms are equipped for hygiene measures and social distancing. Kindly contact reception@lawtonsafrica.com for bookings.* **BANKING DETAILS:** Our banking details have not changed. Any advice of amended bank details that appears to come from our offices should be ignored and reported to us. If in doubt, kindly confirm our banking details telephonically with us before effecting any payment. If we change our banking details in future, a formal notification will be sent to you in advance of such change. It is the responsibility of the payor to verify the bank details before any payments are made. Payments made into a fraudulent bank account not received by Lawtons, will not absolve the payor from liability to Lawtons if verification of the said bank details was not done by the payor prior to payment. Lawtons Inc. practicing as Lawtons Africa, their respective directors, employees and consultants shall have no liability to you arising from or in connection with this email or any attachments. **CONFIDENTIALITY:** This email contains confidential information. It may also be legally privileged. Interception of this email is prohibited. The information on this email and attachments (if any) is only for the use of the intended recipient. If you are not the intended recipient, any disclosure, copying and/or distribution of the content of this email, or the taking of any action thereon, is strictly prohibited and you are requested to delete the email immediately. Should you have received this email in error please notify us immediately by return of email in order for us to ensure it reaches the intended recipient.

PERSONAL INFORMATION:

You may not add the sender's contact details to a database for purposes of direct electronic marketing without their express consent.

Lawtons Africa processes Personal Information in accordance with the Protection of Personal Information Act 4 of 2013 (POPI). Any Personal Information contained in this message may only be Processed in accordance with POPI and any other applicable Data Protection Legislation.

When Processing Personal Information contained in this message, you undertake to comply with all applicable laws, including POPI and any other applicable Data Protection Legislation and applicable industry codes of conduct to the extent that they regulate or relate to the Processing of Personal Information. You further undertake not to do anything, or omit to do anything, which will cause Lawtons Africa to contravene any applicable law, including any Data Protection Legislation.

You will not transfer Personal Information contained in the message to any third party or allow the Processing of Personal Information by a third party without the express written consent of Lawtons.

You will not transfer or Process Personal Information contained in the message outside of the Republic of South Africa without the prior written consent of Lawtons.

You hereby indemnify and hold Lawtons harmless against any and all claims or loss arising from a breach of this Policy and/or arising from the unauthorised Processing of, access to, use and/or disclosure of any Personal Information contained in the message by you.

You agree to provide Lawtons with all assistance and co-operation requested by Lawtons in relation to any requests of complaints received from any person or entity.

You agree to immediately notify Lawtons where there are reasonable grounds to believe that any Personal Information contained in the message has been accessed or acquired by an unauthorized person.

Log-on notice – daily acceptance by staff	**Important Notice** This system is for the use of authorised users only. Unauthorised users will be prosecuted. If you are unauthorised, end this session with immediate effect. Click OK to accept these terms and the firm's privacy policies in relation to processing of Personal Information.
Data privacy notice in engagement letters and brief to counsel	Updated
3rd parties that access floors – Assign, Shred-it, Pest Control, Auditors, Marketing, VIP	Will be provided to Maintenance and Services teams
Advocates briefs to be updated	Updated

UNDERSTANDING THE POPI ACT

10 FAQs answered

1 WHAT IS THE POPI ACT?

The POPI Act is a code of conduct for all businesses.

It encourages the protection of personal information that is processed by public and private bodies.

To do this, the Act will introduce conditions that businesses will be required to comply with when processing personal information.

2 WHEN WILL IT BE IMPLEMENTED?

While the Act hasn't been implemented just yet, it's fair to assume that it will be *some time* this year.

In a briefing on 13 February 2017, advocate Pansy Tlakula said that the POPI Act would only come into operation once the Regulator was fully operational.

It was expected that the Regulator would be up and running around December 2018.

3 WHAT IS PERSONAL INFO?

In terms of the Act, personal information is data that can be used to identify a person.

It is defined as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person."

4 WHO WILL BE AFFECTED?

Put simply — just about everyone.

All companies will be affected by the Act, but in particular, companies that deal with a large amount of personal information — think banks, insurance companies, medical aids, etc.

However, all companies need to have systems in place to deal with personal information.

5 HOW WILL THE POPI ACT AFFECT MY BUSINESS?

THE WAY YOU MANAGE INFORMATION

You'll need to classify consumer data you have and identify if it's 'personal'.

Plus, you'll have to identify records and any sensitive consumer information you have.

THE WAY YOU NOTIFY STAKEHOLDERS

Third parties will have to be notified ASAP if there is a privacy breach and personal information is compromised.

6 WHY SHOULD I COMPLY?

Well, for starters — it's the law.

Also, there are other benefits to complying with the Act.

According to POPI.biz, consumer studies have shown that in 90% of cases, consumers would rather do business with companies that are transparent and comply with legislation than any other business.

Let that sink in.

7 ISN'T THE POPI ACT THE SAME AS THE GDPR?

Sort of, but not really.

It's best to think of them as different flavours of the same thing.

To sum it up, if you're GDPR— (that's General Data Protection Regulation, for those of you living under a rock) compliant — you're pretty much POPI-compliant.

8 DO MARKETERS NEED TO GET PERMISSION TO MARKET TO PEOPLE ALREADY ON THEIR DIRECT MAILING LISTS?

NO.

"If a marketer told me when they collected my information that they are going to use it to send me specials, then gave me the opportunity to unsubscribe every time I got the email — there is that unsubscribe at the bottom — then they're also fine."

- Elizabeth De Stadler, founder of consumer and data protection consultancy Novation.

9 WHAT HAPPENS IF I DON'T COMPLY?

For less serious offences, like hindering an official that is trying to execute a search and seizure warrant, the maximum penalty would be a fine, imprisonment for up to 12 months or a combination of the two.

For more serious offences, the maximum penalties are a R10-million fine or imprisonment for a period of up to 10 years — or a combination of both. YIKES.

10 IS THERE OTHER LEGISLATION IN SA THAT REGULATES PRIVACY?

While POPI is expected to be the primary legislation when it comes to dealing with the protection of information, it certainly won't be the only one.

Other Acts regarding the protection of personal information will have to comply with the principles set out in the POPI Act. This means that **all existing legislation** will have to be amended to ensure compatibility.

The biggest changes in regards to other Acts will be as follows:

- **The Electronic Communications and Transactions Act's** privacy provisions will fall away (where there are duplications of POPI).
- **The Promotions of Access to Information Act** will see all sections dealing with a person's own personal information fall away and be dealt with in POPI.
- **The National Credit Act and Consumer Protection Act** will be amended and will see all sections dealing with privacy removed and dealt with in POPI.