PRIVACY TOOLKIT FOR THE TOURISM INDUSTRY

SATSA

The Voice of Inbound Tourism

VERSION 1 | 24TH NOVEMBER 2020

Introduction

President Cyril Ramaphosa announced that the implementation date of the Protection of Personal Information Act, Act 4 of 2008 ('POPI' or 'POPIA') will be 1 July 2020. Whilst certain provisions thereof already came into effect in 2014, the balance is now required. There will however be a period of grace of one year until 1 July 2021.

SATSA has developed the Privacy Toolkit for the Inbound Tourism Industry with the main objective to educate the industry on the importance of adhering to South Africa's data protection law as well as the General Data Protection Regulation (or GDPR) which was adopted by the European Parliament in early 2016 and came into effect 25 May 2018.

Both the POPIA and GDPR legislative framework creates compliance requirements for the South African tourism industry to adhere to.

What Constitutes Personal Information or Data

There are various definitions of Personal Information in South Africa. Prior to POPIA, the Acts defining it included the ECT Act and PAIA. The ECT Act and PAIA have the same definition, however, Personal information is differently defined in POPIA. Personal Information relates to information to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

b) information relating to the education or the medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the person; and

h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

There are various definitions of Personal Information in South Africa. Prior to POPIA, the Acts defining it included the ECT Act and PAIA. The ECT Act and PAIA have the same definition, however, Personal information is differently defined in POPIA. Personal Information relates to information to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

b) information relating to the education or the medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the person; and

h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Personal Data - What are you collecting?

Examples of the types of personal information that you could collect

Passport / Driver's License

- Name
- Date of birth
- Address
- Email address
- Telephone number
- ID Details
- Race/ethnic orientation (Special category)

Marketing / Communication

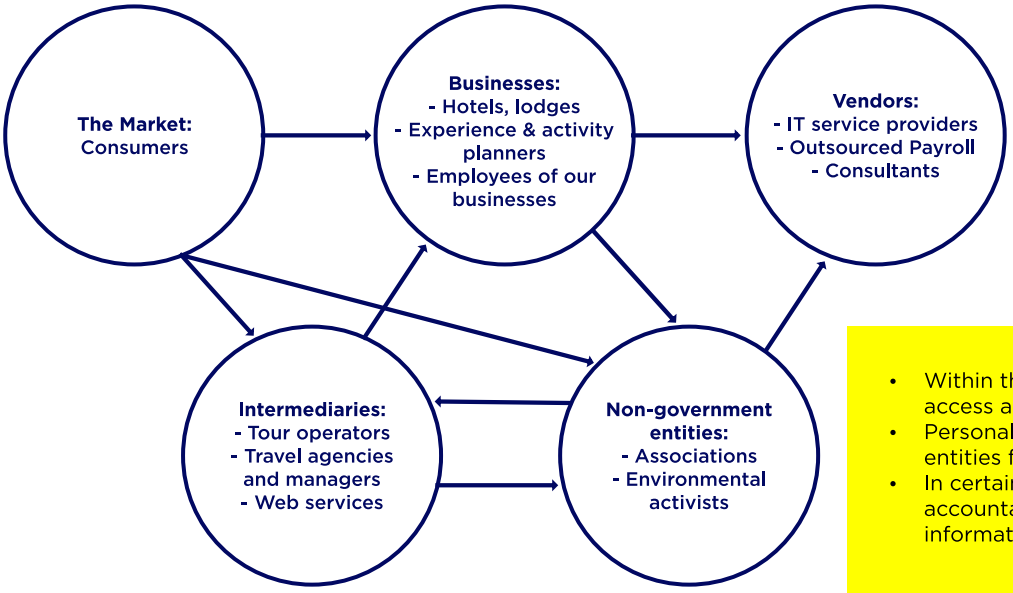
- Email
- Telephone numbers
- IP addresses
- Personal preferences such as travel patterns, like/dislikes

Financial Data

- Financial and payment information

Data Subjects Of The Industry

Data subjects are individuals whose personal information is processed by organisations



- Within the industry, various stakeholders' access and process personal information.
- Personal information is shared among entities for various reasons.
- In certain instances we may share accountability to protect personal information.

The Protection of Personal Information Act (PoPI or POPIA)

Essentially, the purpose of the Protection of Personal Information Act (POPIA) is to protect people from harm by protecting their personal information, to stop their money being stolen, to stop their identity being stolen, and generally to protect their privacy, which is a fundamental human right. To achieve this, the Protection of Personal Information Act sets conditions for when it is lawful for someone to process someone else's personal information.

It does this by regulating the flow of information, advancing the rights of individuals to access the information and by creating 8 conditions or minimum thresholds. It will require both public and private bodies to comply with the conditions when collecting, processing, storing and sharing personal information. South Africa's data protection law was enacted in 2013 but has yet to commence. The POPI commencement date or POPI effective date will not be before the Information Regulator is operational, which might only be in 2020.

Customer-Service Requirements of the POPIA

The Protection of Personal Information Act involves three parties who can be natural or juristic persons:

(a) The data subject: the person to whom the information relates.
(b) The responsible party: the person who determines why and how to process. For example, profit companies, non-profit companies, governments, state agencies and people. Called controllers in other jurisdictions
(c) The operator: a person who processes personal information on behalf of the responsible party. For example, an IT vendor. Called processors in other jurisdictions.

The POPIA places various obligations on the responsible party, which is the body ultimately responsible for the lawful processing of personal information. Responsible parties should only use operators that can meet the requirements of lawful personal information processing prescribed by the Protection of Personal Information Act.

The 8 Conditions or Minimum Thresholds of POPIA

1. Accountability — Companies will be accountable for complying with the measures prescribed in the Act. These measures, such as fines or imprisonment, make the company responsible and liable for the personal information from the moment it is collected to the time of its deletion.
2. Purpose Specification — Information can only be collected for a legitimate and lawful purpose. Companies may not keep the information for a period longer than that which is required to fulfil their purpose.
3. Processing Limitation — Companies will only be permitted to collect the minimum information required for their purpose. This condition includes the responsibility to get proper consent from the individual, ensure the individual is aware that their data is being processed and for what purpose.
4. Further Processing Limitation — This condition limits any secondary use of the information, meaning that the information cannot be used for any other purpose than the purpose for which it was collected initially.
5. This includes preventing the disclosure or transfer of personal information to third parties.
6. Information Quality — Companies will have to take practical steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.
7. Openness — Companies will be required to clearly inform the individual that information is being collected on them, the reasons for collecting and what the information will be used for.
8. Security Safeguards — Companies will have to implement security measure to ensure the security, integrity and confidentiality of the information collected. This will include taking technical measures to prevent loss, damage and unlawful access.
9. Data Subject Participation — Individuals have the right to ask and be given the details of any information that has been collected on them at no cost.

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since the Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.

The GDPR mandates that EU visitors be given several data disclosures. The site must also take steps to facilitate such EU consumer rights as a timely notification in the event of personal data being breached. Adopted in April 2016, the Regulation came into full effect in May 2018, after a two-year transition period.

Customer-Service Requirements of the GDPR

GDPR aims to "harmonise" data privacy laws across Europe as well as to give greater protection and rights to individuals within the EU. It will require companies covered by the GDPR to be more accountable for their handling of people's personal information by having data protection policies, data protection impact assessments and relevant documents on how data is processed.

Under the rules, visitors must be notified of data the site collects from them and explicitly consent to that information-gathering, by clicking on an Agree button or other action. Sites must also notify visitors in a timely way if any of their personal data held by the site is breached. These EU requirements may be more stringent than those required in the jurisdiction in which the site is located.

In what ways is POPIA different to GDPR

The GDPR applies to the personal data of EU data subjects (in short, EU citizens), regardless of jurisdiction or where the data is being processed. POPIA on the other hand is only limited to personal information processed within the borders of South Africa. POPIA only defines two key roles which an organisation may take — responsible parties (controllers) and operators (processors). The GDPR understands that these two roles alone are not sufficient definitions and recognises that there are additional distinct roles such as joint responsible parties. It is clear from the definition above that POPIA and GDPR overlap in nearly all areas.

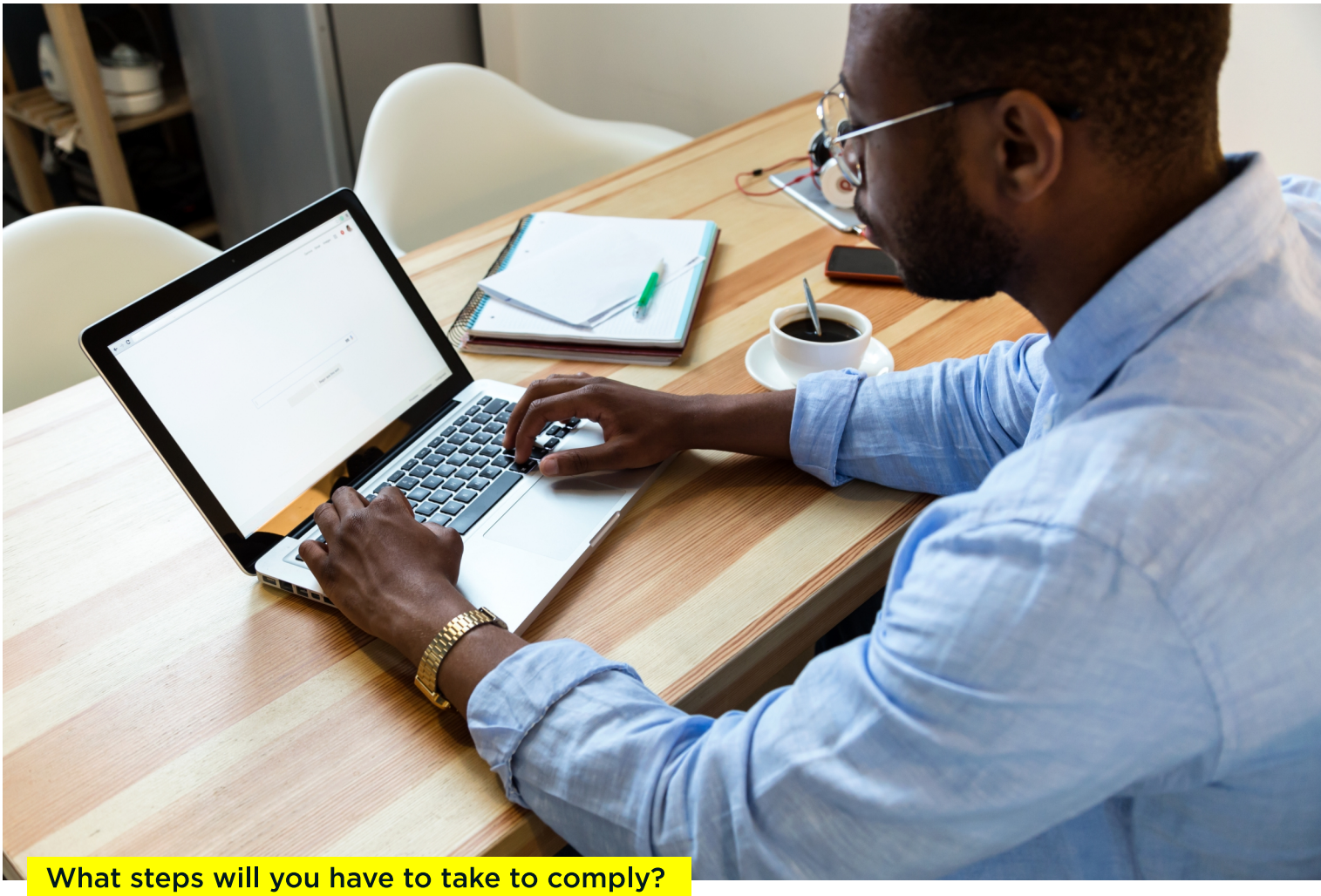
The GDPR does not protect legal entities. It also does not create such serious penalties for failing to protect an account number. It exempts some SMEs from having to keep records. SMEs can find a useful infographic for SMEs on the website of the European Commission. The GDPR also makes it obligatory for some organisations to have a data protection officer, whereas POPIA provides that every organisation has an information officer by default.

The GDPR has a definition of genetic data and requires data controllers to do data protection impact assessments. The fines are much bigger in the GDPR but there are no criminal offences in the GDPR. The GDPR's fine of €20 million or 4% of a company's global turnover, is much larger than that of POPIA's R10 million. The POPIA further envisions the possibility of criminal sanctions in the event of non-compliance.

As further protection for consumers, the GDPR also calls for any personally identifiable information (PII) that sites collect to be either anonymized (rendered anonymous, as the term implies) or pseudonymized (with the consumer's identity replaced with a pseudonym). The pseudonymization of data allows firms to do some more extensive data analysis, such as assessing average debt ratios of its customers in a region, a calculation that might otherwise be beyond the original purposes of data collected for assessing creditworthiness for a loan.

Compliance with the GDPR should result in near perfect compliance with POPIA. The requirements for controllers and processors as set out in POPIA are very closely aligned to the various roles set out in the GDPR but at this point in time, POPIA does not consider the other relationships, however these may be included in future regulations.

Considering the EU is one of South Africa's biggest trade partners, South Africa is going to have to bring POPIA more in line with the GDPR. This could be done by Parliament amending POPIA or the Information Regulator interpreting it in line with the GDPR or publishing Regulations that are in line with the GDPR. The GDPR applies to any data processing activities that are done by a controller in the EU. It also applies to all processing of personal data of data subjects residing in the EU even if the entity processing the data is not in the EU. So, if any entity is offering goods and services to EU citizens, they will be required to comply with the GDPR.



What steps will you have to take to comply?

1. Appoint an Information Officer to account for privacy formally.
2. Draft a Privacy Policy to implement manual controls.
3. Raise awareness amongst all employees of their roles in protecting personal information.
4. Know where personal information is processed in your organisation
5. Amend contracts with operators.
6. Report data breaches to the regulator and data subjects.
7. Check that they can lawfully transfer personal information to other countries.
8. Only share personal information when they are lawfully able to.

Managing Privacy Risk Controls for The Entire Lifecycle of Personal Information

Stage 1. Collect/create personal Information

Stage 2. Utilise

Stage 3. Store

Stage 4. Share/Transfer

Stage 5. Archive

Stage 6. Destroy

Stage 1. Collect/create personal Information

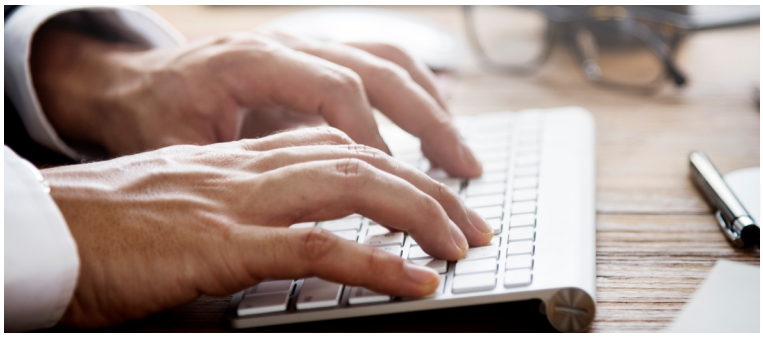
- Collect only what is required
  - Know why you need specific information and document the decision.
  - Remove the fields on systems or forms for information that isn't required to properly deliver your service offering.
- Communicate how you handle personal information
  - Include a short notice on terms and conditions or application forms.
  - Maintain a Privacy Notice on your website that sets out how your company handles personal information. Make sure what you state is true.
  - Ensure that your employees are aware of your information handling processes so that they are able to answer questions that customers may ask. For example, a guest may ask why their passport or credit card details are taken – you must be able to answer clearly that ID/ passport copies are required in terms of the immigration Act and for health and safety reasons. Credit card details are taken in case of charges that are not settled.
- Get consent from a person when:
  - You'd like to direct market to them.
  - You want to share their contact details with a party that is not directly involved in the offered service.

Stage 2. Utilise

- Our industry generally collects and save a large amount of information on clients including contact details, history, personal preferences, birthdays etc. What can/can't be kept?
  - The differentiator for 5-star guest treatment is understanding their preferences to the extent that the experience they receive is tailored. Provided the information collected is relevant to a specific service/ experience offering and the guest is aware that the information is collected, there is generally no risk.
  - If a guest has not returned in for example 5 years, the information held would probably be outdated; and should be deleted.
  - Regular guests are likely to prefer having their information available when they return to avoid completing the same forms and to have a unique experience.
- How should this be kept?
  - If personal information about a guest is relevant it must be kept securely.
  - For example, information should be kept in a system that is access controlled.
  - Sometimes paper documents are necessary, especially when checking guests in and handing over shifts. However, all documents that contain personal information (such as ID/ passport copies, credit card details etc.) must be stored securely in a locked cabinet and thereafter in a vault for safe keeping.
  - Ideally information should be kept electronically to avoid the risk of papers lying about.

Stage 3. Storing Personal Information

- Store personal information on a secure platform e.g. avoid paper storage where you can and use a central system to reduce copies of information that may be altered or outdated.
- Only store what is required – remember the less you collect and store, the lower the risk of the information being lost, stolen or otherwise misused.
- There is legislation that requires storage of personal information for certain periods of time
- Generally, the following periods apply:
- Keep employee information for 4 years after they leave the organisation.
- Keep financial information for 7 years.
- Keep customer information in line with the immigration Act and health and safety requirements.
- If information is used in an investigation or proceeding, keep it for the period that it is actively used and then (after) apply the retention period.
- When storing personal information, access to this information must be secure. Locked away in cupboards and in locked offices or storage facilities.



Stage 4. Sharing personal Information

- Only share personal information that is absolutely required to deliver on a committed service or contract requirement.
- Verify that you are sharing personal information with the correct persons. For example, always check the recipient field in an email to make sure that the correct person(s) receive the information. Don't share personal information with persons that don't need access to it.
- Before sharing personal information with employees, make sure that their employment contract has specific confidentiality clauses and that they have acknowledged understanding thereof.
- Before sharing personal information with an external party, ensure that there is a signed contract that sets out confidentiality and data protection requirements.
- Accountability for protection of information cannot be shared with third parties
- Personal information must be shared securely. For example, this can be done on a central internal system instead of using USBs and other removable devices.
- When sending personal information externally, apply password on the document and send the password in a different mechanism. Alternatively, use a secure file transfer protocol (SFPT) – Refer to your IT team or supplier for assistance.
- Direct marketing can be done in the following instances - where the option to opt out is available:
  - To existing customers that have not opted out
  - To potential customers where it is the first time the organization reaches out with direct marketing, asking for consent to market
- The controller cannot automatically tick an electronic opt in box as "yes", the consumer must have a choice.
- Provision of services may not be subject to consumers opting into direct marketing.
- When sending various forms of direct marketing, the consent indicators for each form of communication must be maintained.
- Newsletters should also be sent with the option to opt out, to make it easier to manage your consumer preferences.
- When using an external company to do mass mails and SMS using their own contact details, ensure that you have assurance that they only send to consumers that have not opted out of receiving direct marketing communication.
- Third parties that normally have access to personal information include:
  - IT service providers/ support
  - Outsourced payroll providers
  - Marketing agencies
  - Security services
- Ensure that all external parties that access personal information are bound by a contract that also specifies privacy and security requirements
- Additional due diligence should be conducted for external parties that have high volumes of access to personal information.
- This includes asking them to provide assurance in terms of GDPR article 28 as well as other security safeguards.
- Phishing
  - A malicious scam targeting an individual or group via email, text or call
  - The aim is to appear like a legitimate business or email, website
  - Normally warning messages or prompts to reset login details
  - Credentials are then stolen and used for various credential-based attacks like logging into profiles online where you may have used the same passwords.
  - Remember, never use the same password for multiple platforms

The 3 types of phishing emails

Clone Phishing

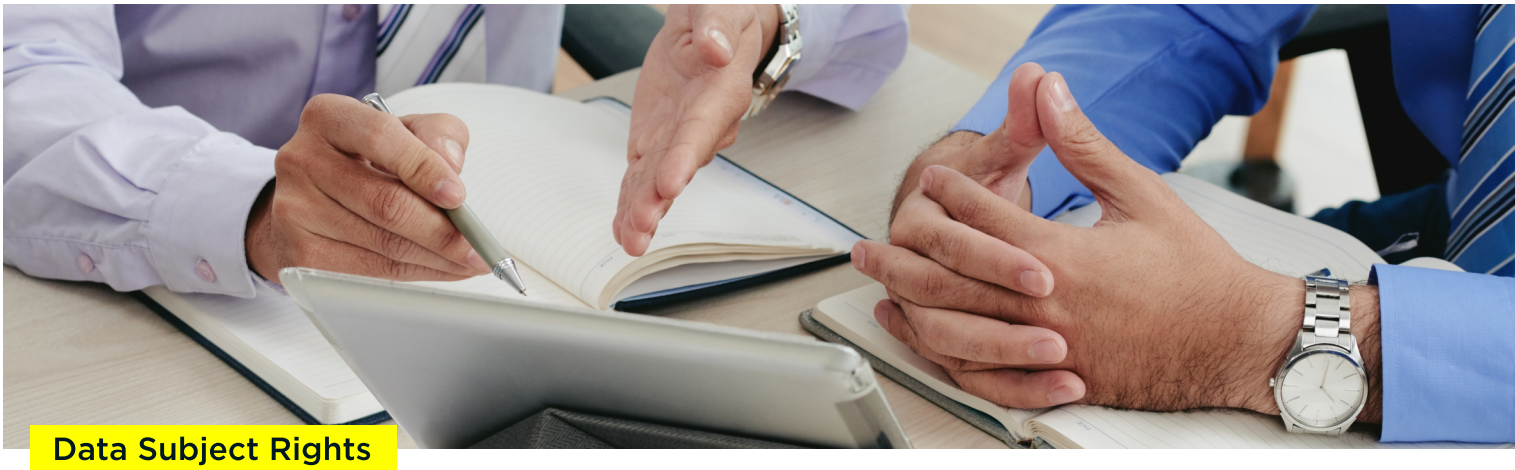
Clone Phishing is where a legitimate, and previously delivered, bit of online correspondence is used to create an almost identical or "cloned" email.

Spear Phishing

Spear Phishing is a phishing attempt directed at a particular individual or company.

Whaling

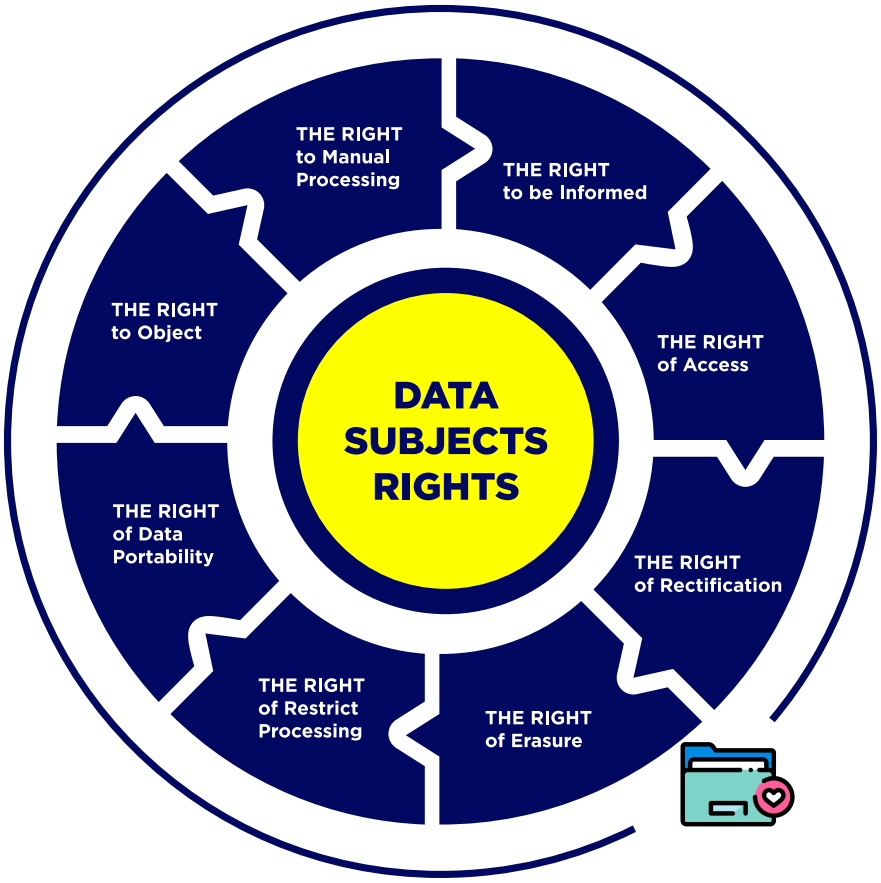
Whaling is a phishing attempt directed specifically at a senior executive or another high-profile target within a business.



Data Subject Rights

Every person has certain rights in relation to their personal information

- A company should have a process to manage data subject rights requests.
- For South African companies, the Promotion of Access to Information Act (PAIA) provides persons the right to request access to their personal information. Companies are required to maintain a PAIA Manual on their website and it must also be lodged with the Human Rights Commission.
- There are other data subject rights that should be managed appropriately.



Conclusion

While there are several key differences in the two pieces of legislation, the POPIA can be seen as a steppingstone to GDPR compliance. Inbound Tourism businesses not in compliance with POPIA will not meet the requirements of the GDPR.

Compliance with the GDPR carries a few additional requirements, such as conducting privacy impact assessments and building privacy by design into the fabric of the organization and improving records and bodies of evidence to demonstrate compliance, however compliance with the GDPR will result in majority compliance with POPIA.

Proactive compliance efforts go a long way with customers, strategic partners and regulators. This can be done by conducting an internal assurance test or getting help from a reputable service provider to help you check that you are on the right track.