WHIPPING THE CAT®

TAILORED LEGAL SERVICES

Protection **O**f **P**ersonal **I**nformation

[All your POPI questions answered]

To whom does it apply?

There are very few businesses in South Africa that will not be impacted by POPI.
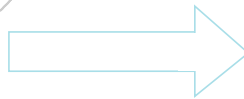
EVERYONE

POPI applies to:

1 Any public or private body or any other person who determines the purpose of and way for processing personal information (**responsible party**).

2 Any person who **processes** personal information for a responsible party.

It includes company personal information

When will it affect me?

Once the Act comes into force and then a compliance grace period of 1 year will apply.

What are your obligations under POPI?

1 Ensure info is relevant and up to date

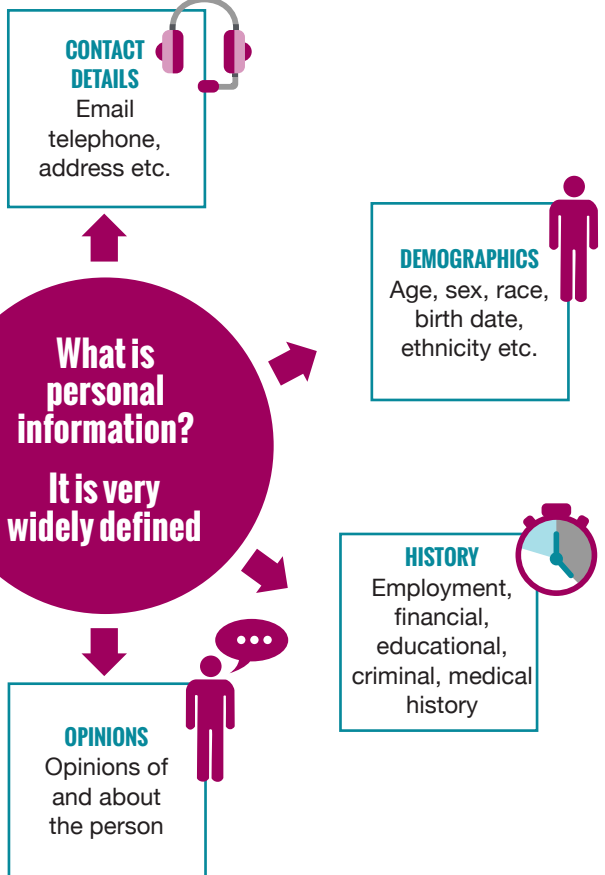**2** Allow the data subject to see their info on request

3 Apply reasonable security measures to protect info

4 Only collect info that you need for a specific purpose

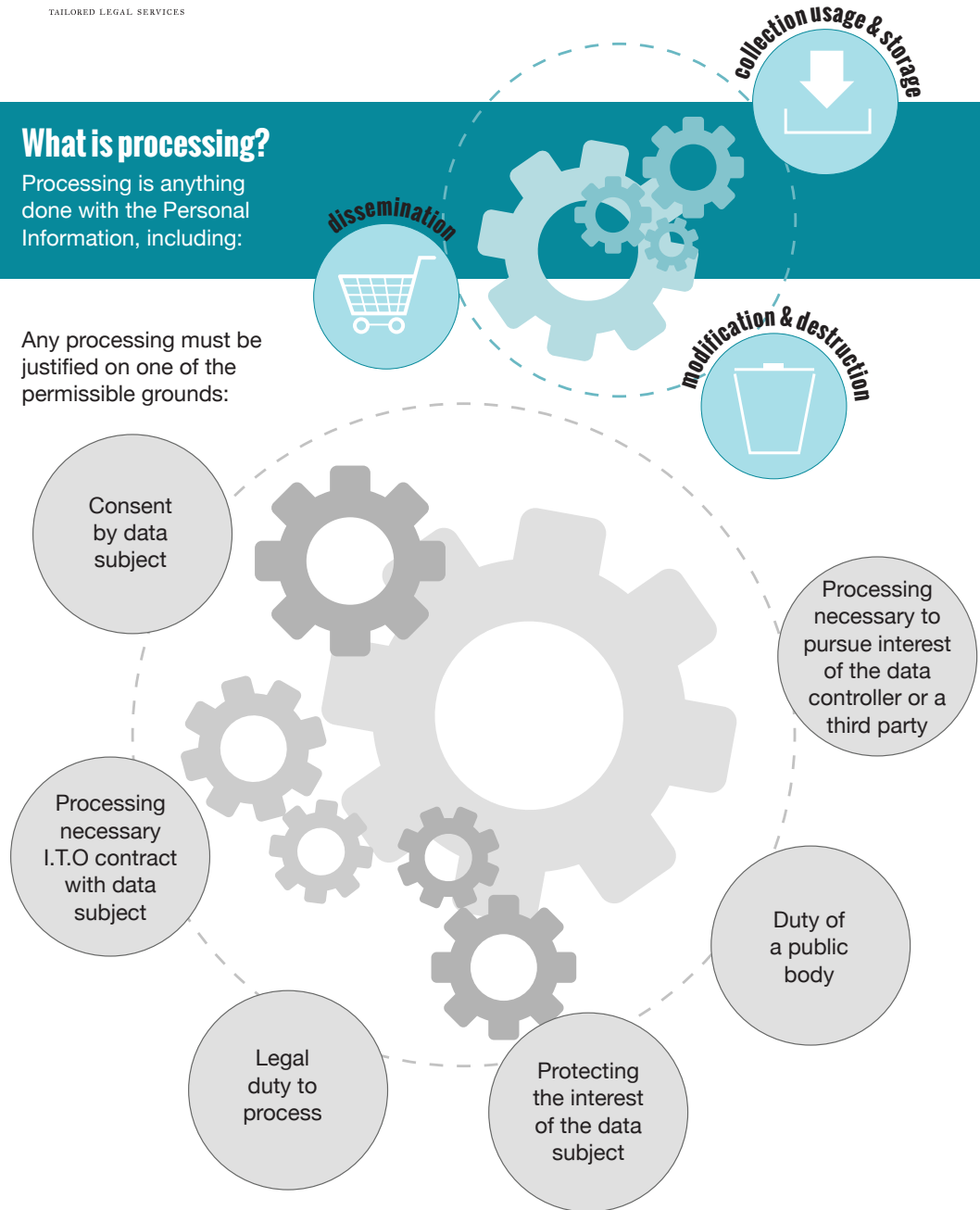**5** Only hold as much info as you need, and only for as long as you need it

CONTACT DETAILS
Email telephone, address etc.

CORRESPONDENCE
Private correspondence

DEMOGRAPHICS
Age, sex, race, birth date, ethnicity etc.

What is personal information?

It is very widely defined

BIOMETRICS
Biometric information, Blood type etc.

HISTORY
Employment, financial, educational, criminal, medical history

OPINIONS
Opinions of and about the person

collection usage & storage

What is processing?

Processing is anything done with the Personal Information, including:

dissemination

modification & destruction

Any processing must be justified on one of the permissible grounds:

Consent by data subject

Processing necessary to pursue interest of the data controller or a third party

Processing necessary I.T.O contract with data subject

Duty of a public body

Legal duty to process

Protecting the interest of the data subject

? **What is special personal information?**

A higher degree of protection is given to special personal information under POPI

information concerning a child

religious or philosophical beliefs

race or ethnic origin

trade union mebership

criminal behaviour

sexual life

dna

political opinions

health

What are the information processing principles?

There are **8** information processing principles which form the core of POPI.

1 **PROCESSING LIMITATION** - processing must be lawful and personal information may only be processed if it is adequate, relevant and not excessive given the purpose for which it is processed

2 **INFORMATION QUALITY** - take steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary

3 **ACCOUNTABILITY** - the responsible party must ensure that the eight information processing principles are complied with

4 **PURPOSE SPECIFICATION** - personal information must be collected for a specific purpose

5 **FURTHER PROCESSING LIMITATION** - this is where personal information is received from a third party and passed on to the responsible party for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was initially collected

6 **OPENNESS** - personal information may only be processed by a responsible party that has notified the Information Protection Regulator. Further certain prescribed information must be provided to the data subject by the responsible party including what information is being collected, the name and address of the responsible party, the purpose for which the information is collected and whether or not the supply of the information by that data subject is voluntary or mandatory

7 **SECURITY SAFEGUARDS** - the responsible party must secure the integrity of personal information in its possession or under its control by taking measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information

8 **DATA SUBJECT PARTICIPATION** - a data subject has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about them and request a copy of it, and request it to be correct destroyed etc.

Can I send personal information overseas?

Yes, but there must be protections in place:
- other country has similar laws
- inter-company / group rules
- contract between data sender and data receiver
- data subject consents
- transfer necessary I.T.O contract with data subject
- transfer is necessary for the benefit of data subject and consent is impractical

Who is the Information Regulator and what are its powers?

The Information Regulator is a body that will be appointed in terms of POPI and can:

educate the public about POPI

Issue codes of conduct and make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct.

monitor and enforce compliance

handle complaints about alleged violations

attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation

For how long do I need to retain personal information under POPI?

Subject to retention periods, you must retain the record for a period which will afford the data subject a reasonable opportunity to request access to the record.
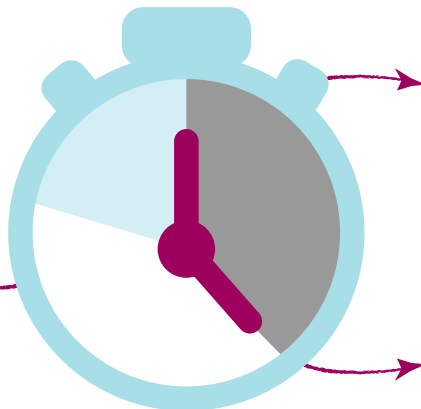
Personal information must not be retained longer than is necessary for achieving the purpose for which the information was collected.

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

DIRECT MARKETING
POPI changes things -
opt-in rather than opt-out

Responsible parties should make use of an opt in system when using electronic communications to conduct direct marketing.

Why should I comply with POPI?

1 POPI promotes transparency with regard to what information is collected and how it is to be processed. This openness is likely to increase customer confidence in the organisation.

2 POPI compliance provides rules for capture and storage to reduce risk of data breaches.

3 Compliance demands identifying Personal Information and taking reasonable measures to protect the data. This will likely reduce the risk of data breaches and the associated public relations and legal ramifications for the organisation.

Q What is the sanction for non-compliance with POPI?

A Reputation damage and a penalty of a **FINE OF R10 MILLION** and / or imprisonment of up to 10 years.