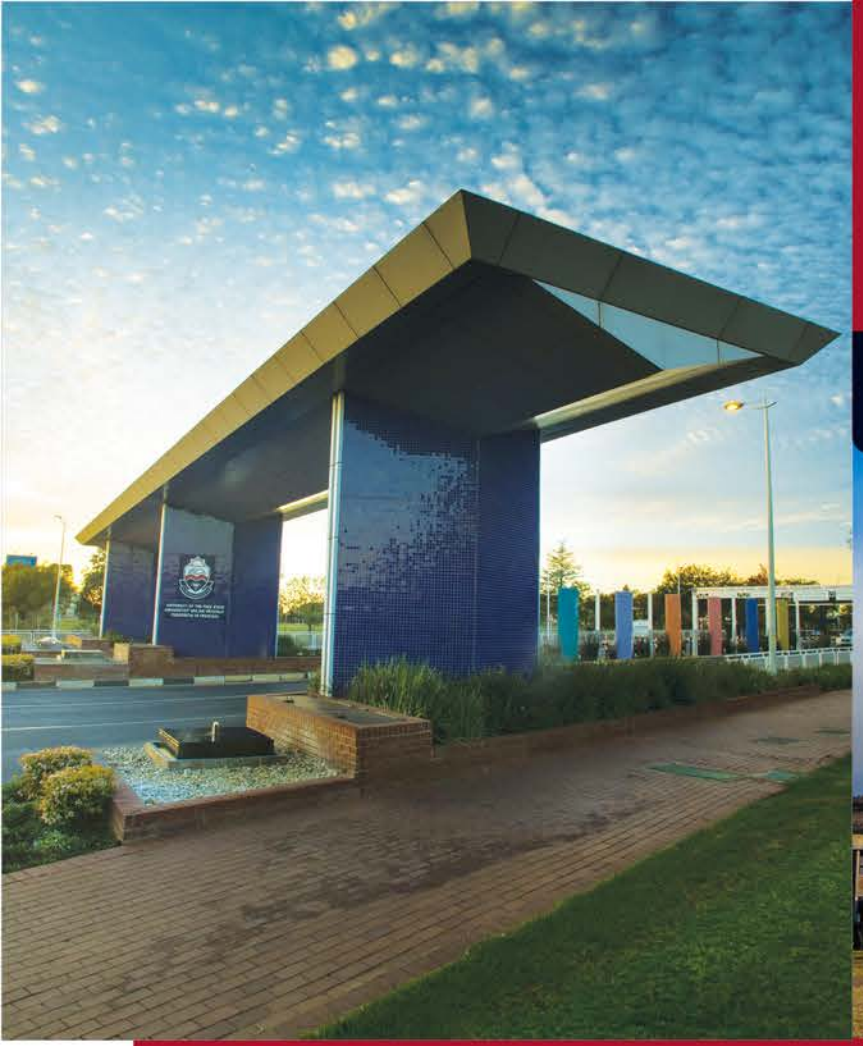


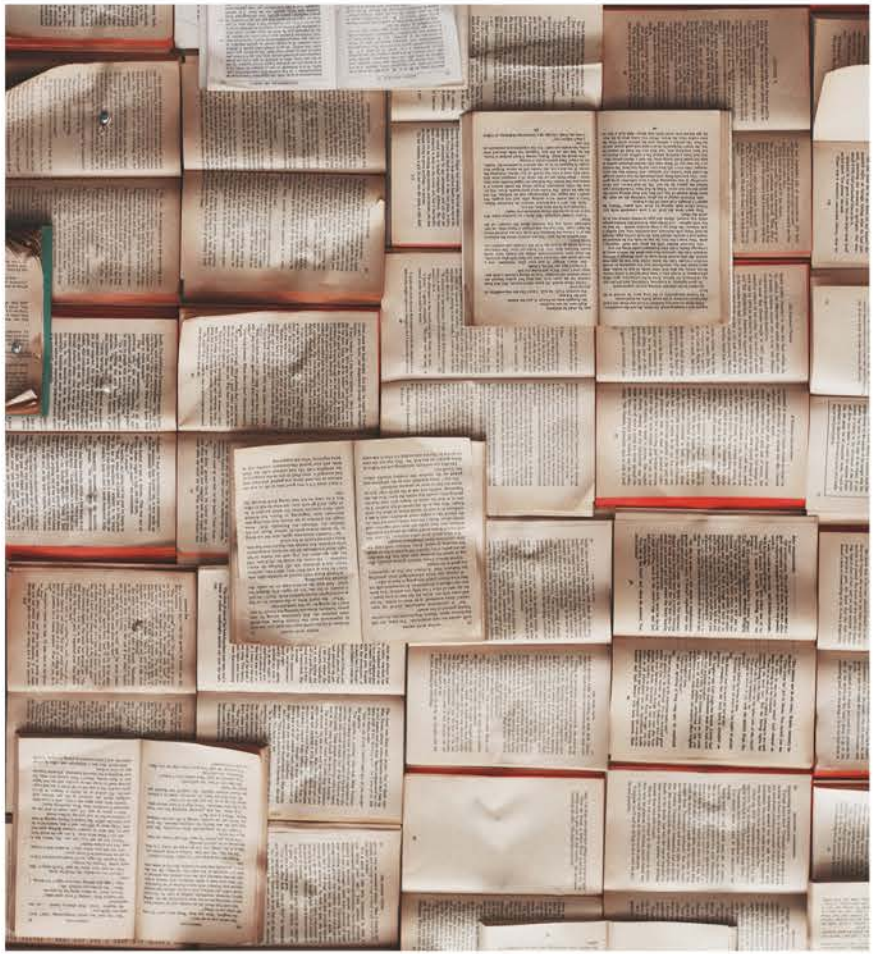
POPIA COMPLIANCE TRAINING
REGISTRAR'S OFFICE
LEGAL SERVICES AND
REGULATORY COMPLIANCE

APRIL 2021

T: +27 51 401 9111 | info@ufs.ac.za | **www.ufs.ac.za**
UFSUV | UFSweb | UFSweb | ufsuv

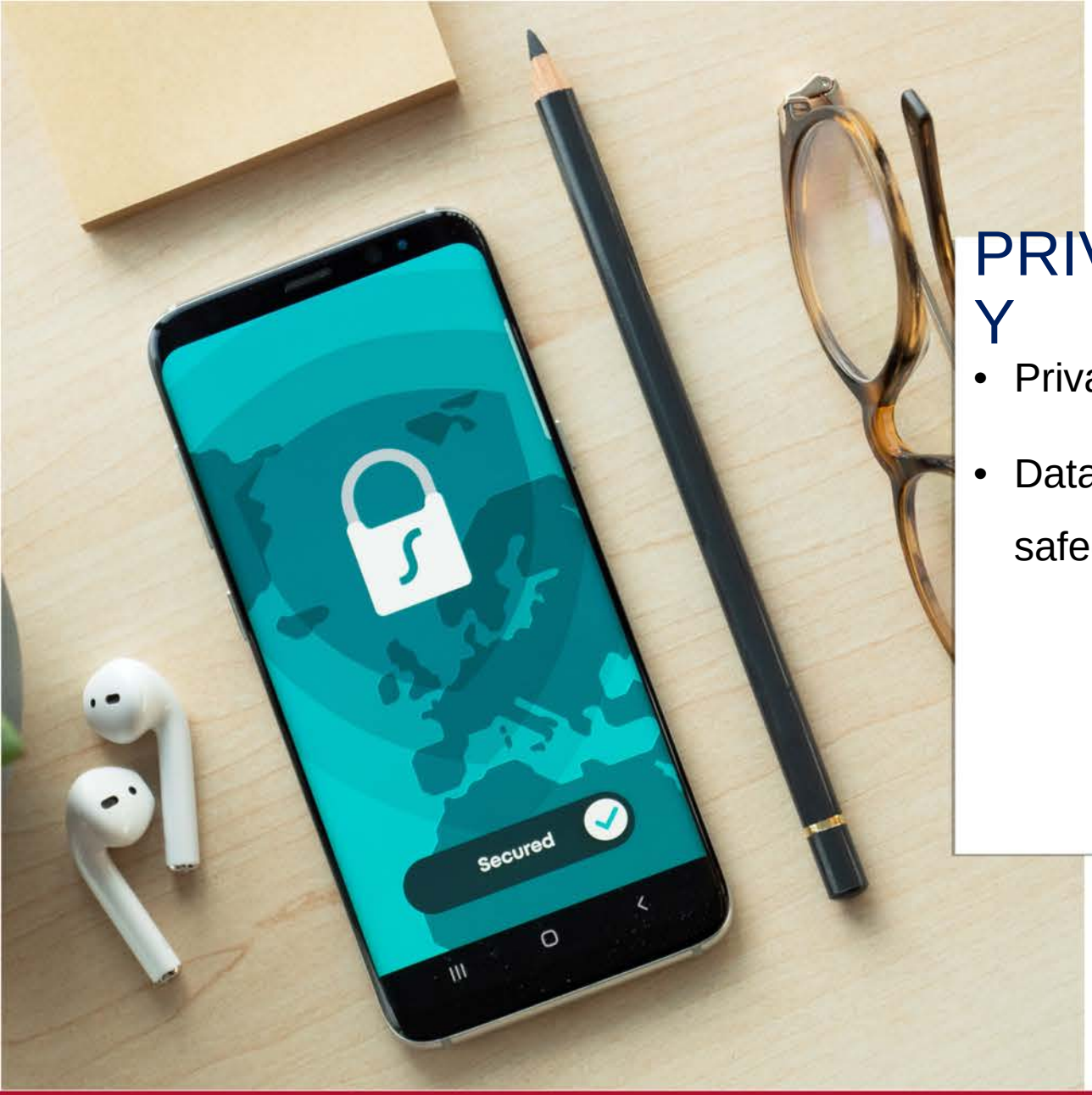
Inspiring excellence.
Transforming lives.

UNIVERSITY OF THE
FREE STATE
UNIVERSITEIT VAN DIE
VRYSTAAT
YUNIVESITHI YA
FREISTATA
UFS



PURPOSE

- The purpose of the Act is to protect privacy and to regulate the use of personal information.
- The essence of information protection is to provide a person with a degree of control over his or her personal information in instances where his or her personal information is being collected, stored, used or communicated by another person or institution.

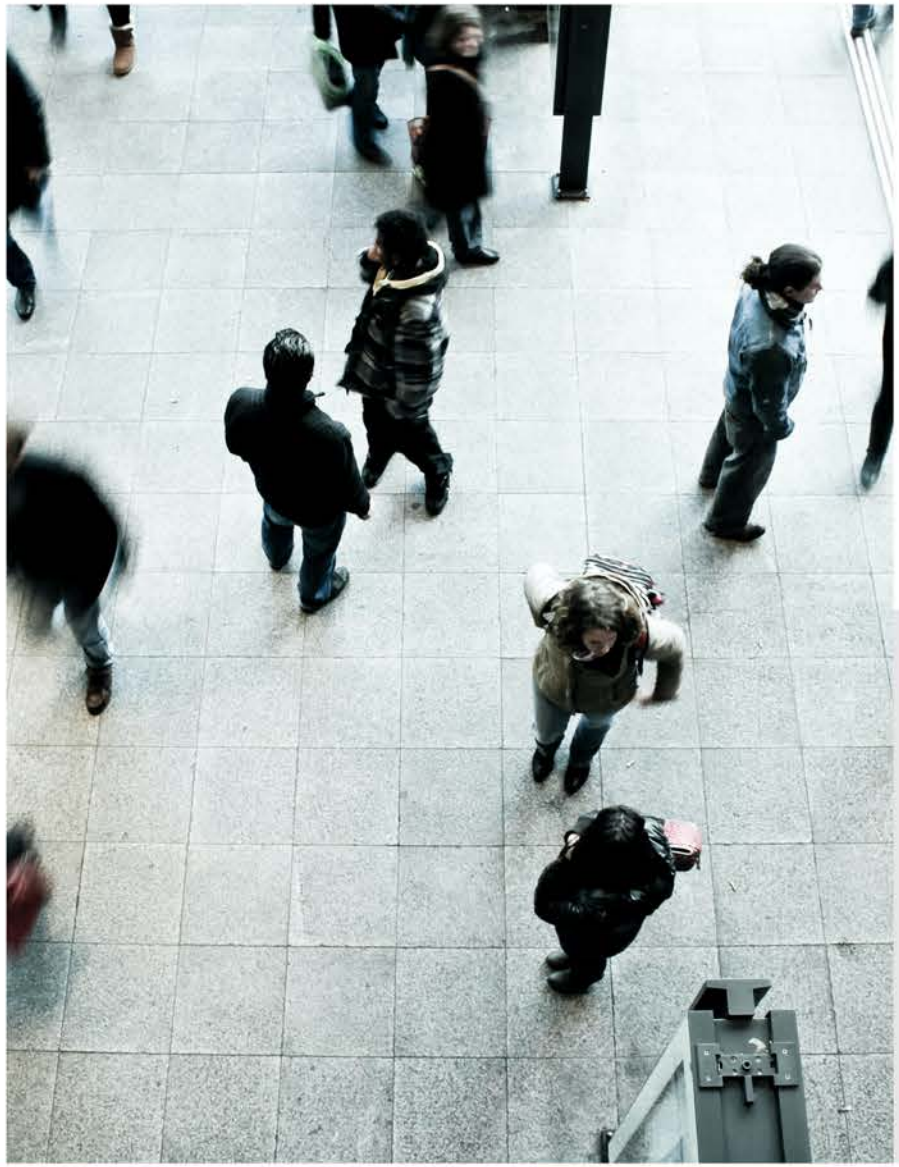


PRIVACY

- Privacy is a valuable aspect of personality.
- Data or information protection forms an element of safeguarding a person’s right to privacy.

FUNDAMENTAL RIGHT

- The recognition and protection of the right to privacy is a fundamental human right and enshrined in the Bill of Rights in the RSA Constitution.



NOT ABSOLUTE RIGHT

- The right to privacy is not an absolute right.

This right has to be weighed against and balanced with other competing rights. In other words – when protecting a person's personal information, consideration should also be given to competing interests such as:-

- The administering of social programmes;
- Maintaining law and order; and
- Protecting the rights, freedoms and interests of others including the commercial interests of industry sectors.

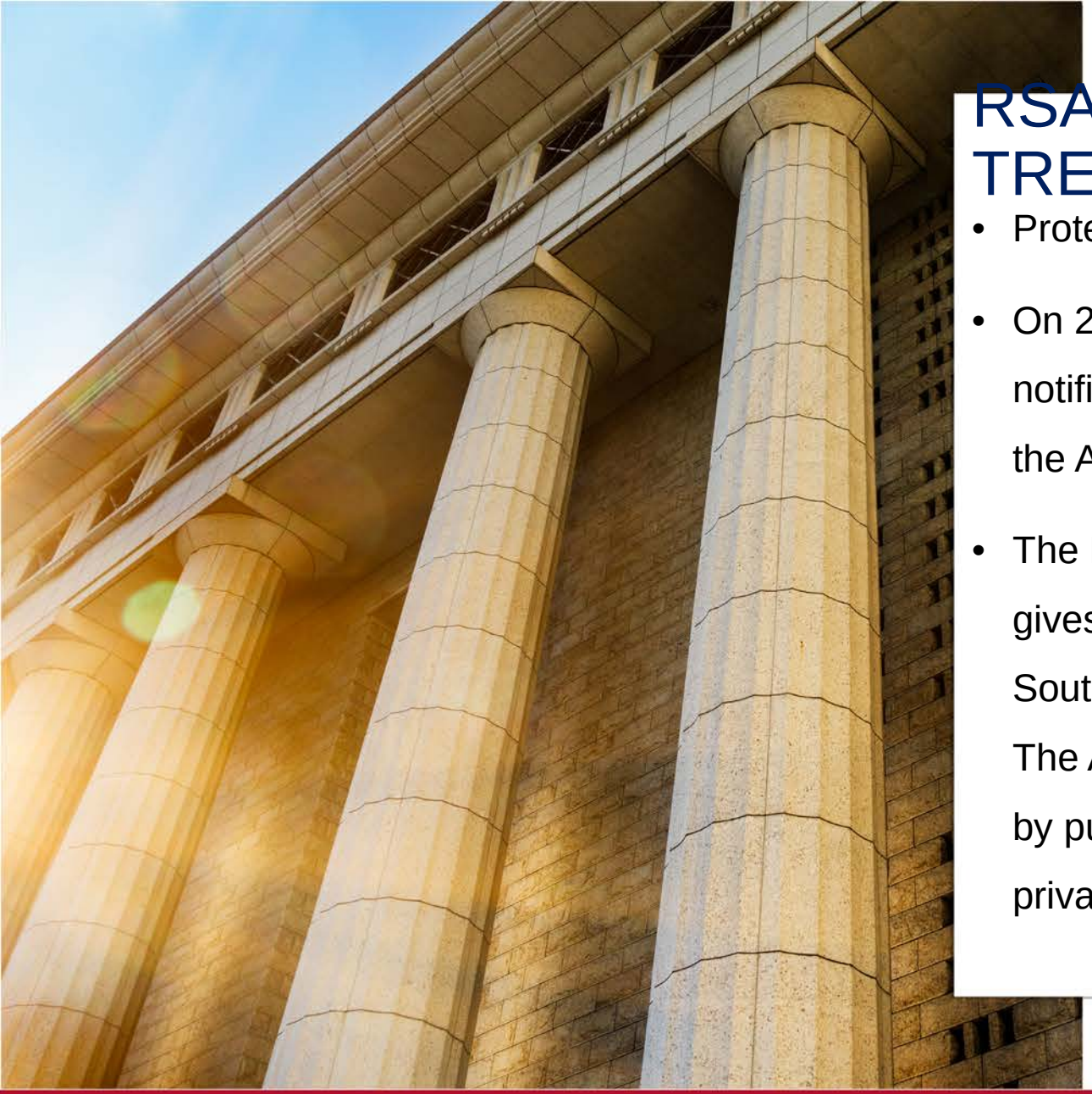
These opposing interests have to balance against each other – a delicate act

- Confidentiality is different to privacy.
- Privacy – Constitutional right which is now entrenched under POPI.
- Confidentiality – Contractual or right permitted under an Act.

CONFIDENTIALITY VS PRIVACY

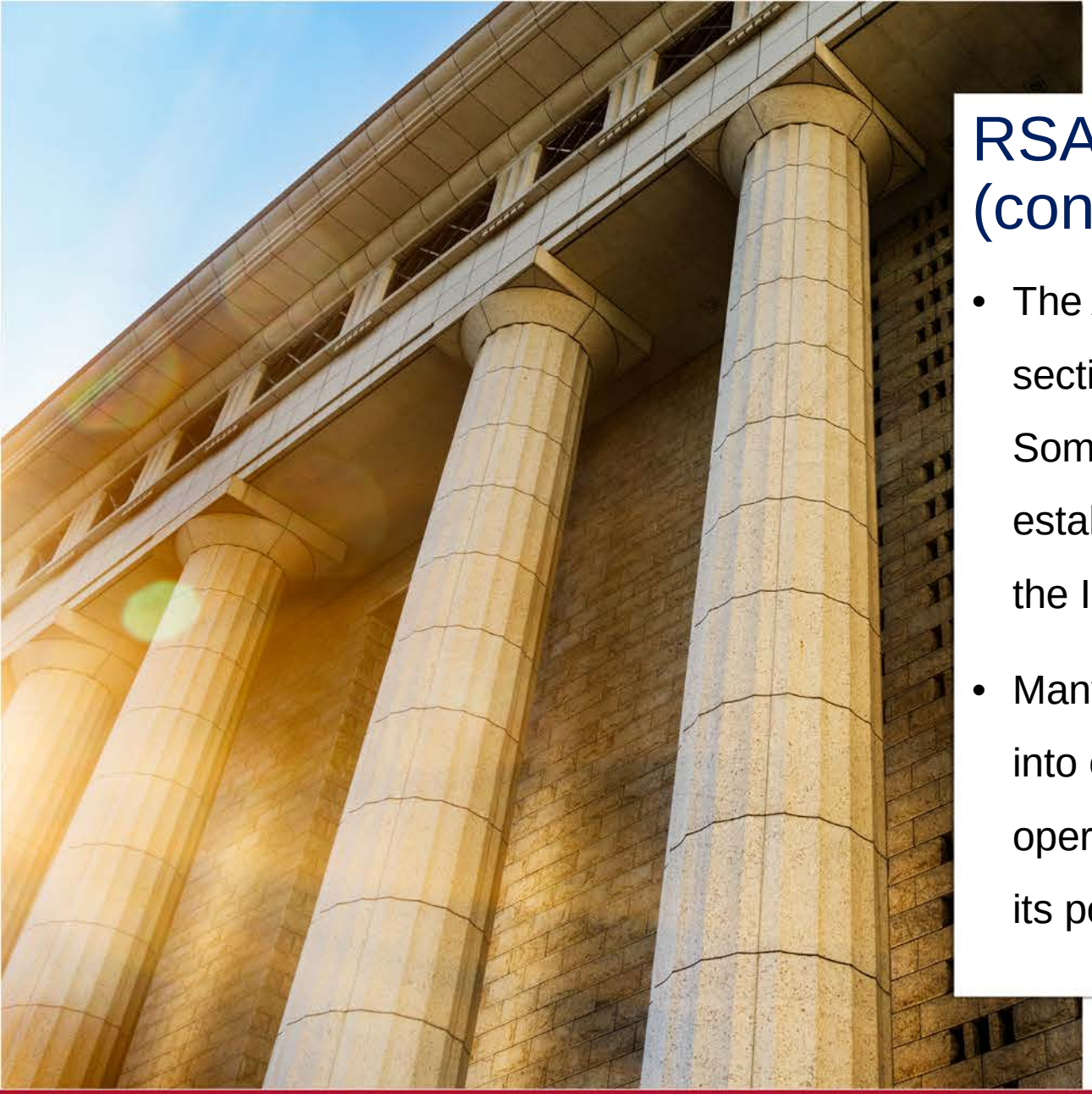
PRIVACY LAWS

- There are now well over 30 countries that have enacted privacy laws or information protection statutes at national or federal level world over.
- This number is steadily growing.



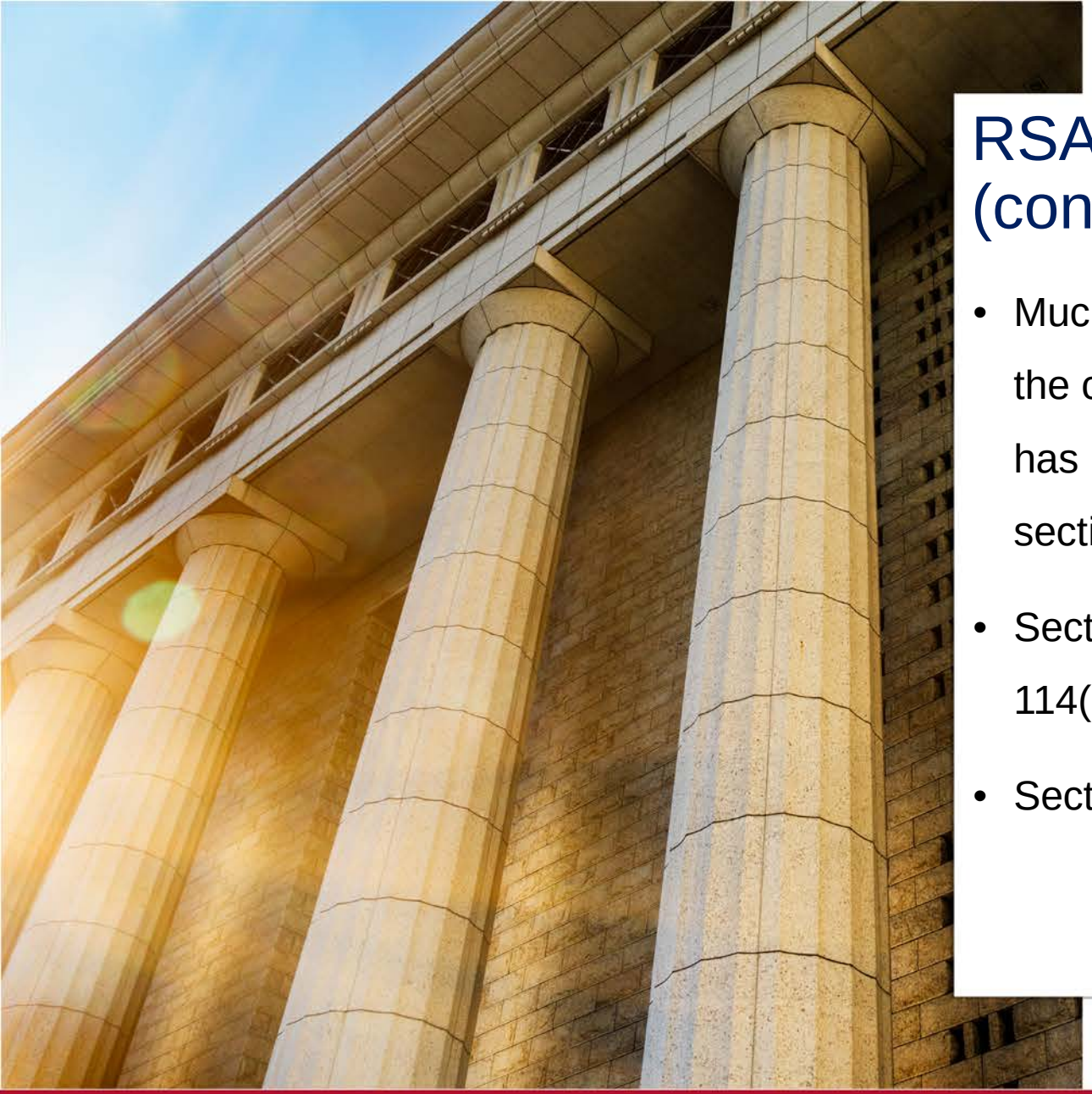
RSA FOLLOWING THE TREND

- Protection of Personal Information Act becomes an Act (POPIA)
- On 26 November 2013 the Government Gazette published notification that the President has assented to POPIA, publishing the Act for general information
- The Protection of Personal Information Act, 2013 (Act 4 of 2013) gives effect to section 14 of the Constitution of the Republic of South Africa which provides that everyone has the right to privacy. The Act promotes the protection of personal information processed by public and private bodies and seeks to balance the right to privacy against other rights, such as access to information.



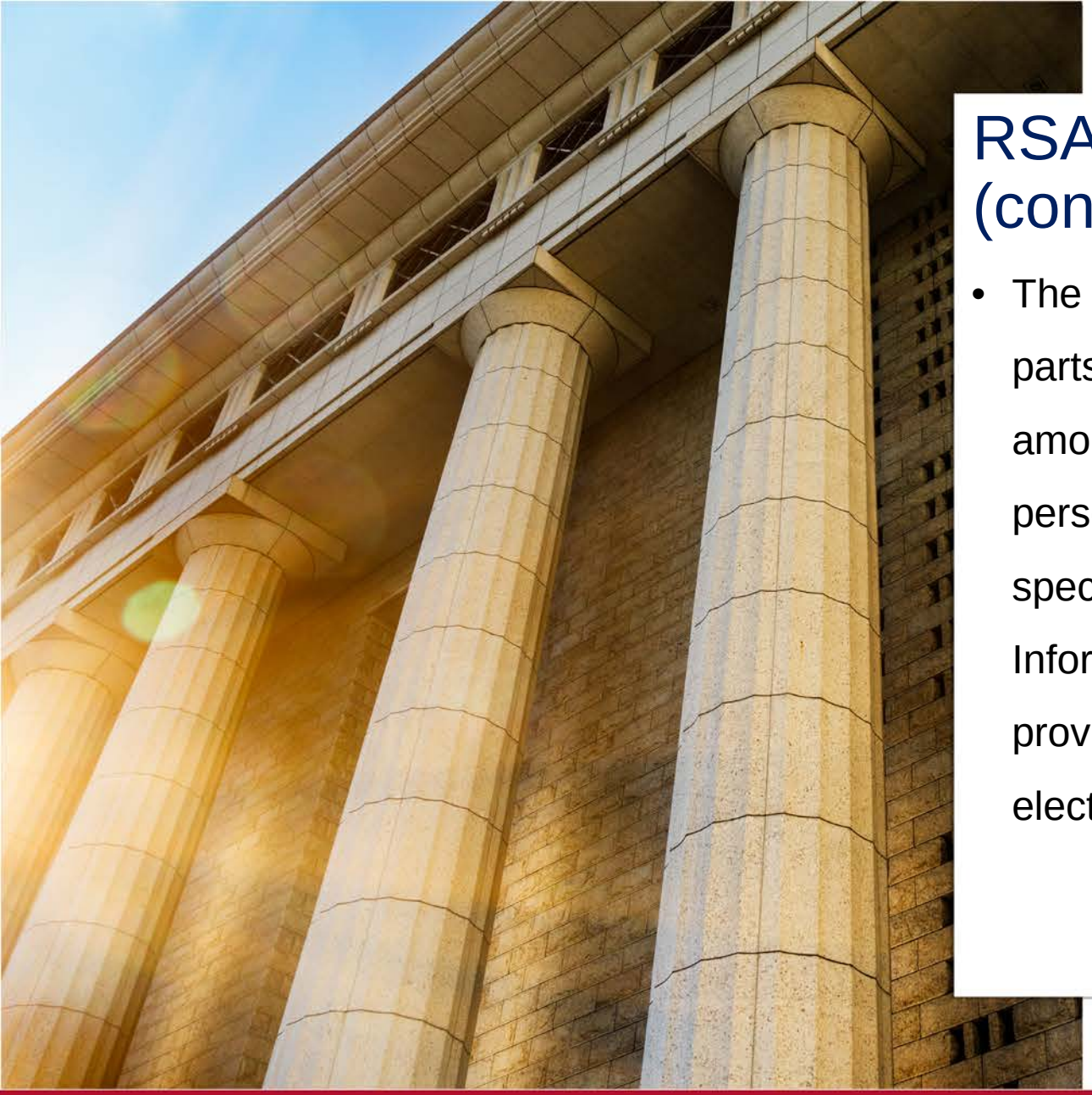
RSA FOLLOWING THE TREND (cont.)

- The Act has been implemented incrementally, with a number of sections of the Act having been implemented in April 2014. Some of the sections include those relating to the establishment of the Information Regulator. The members of the Information Regulator took office on 01 December 2016.
- Many of the remaining provisions of the Act could only be put into operation at a later stage as they require a state of operational readiness for the Information Regulator to assume its powers, functions and duties in terms of the Act.



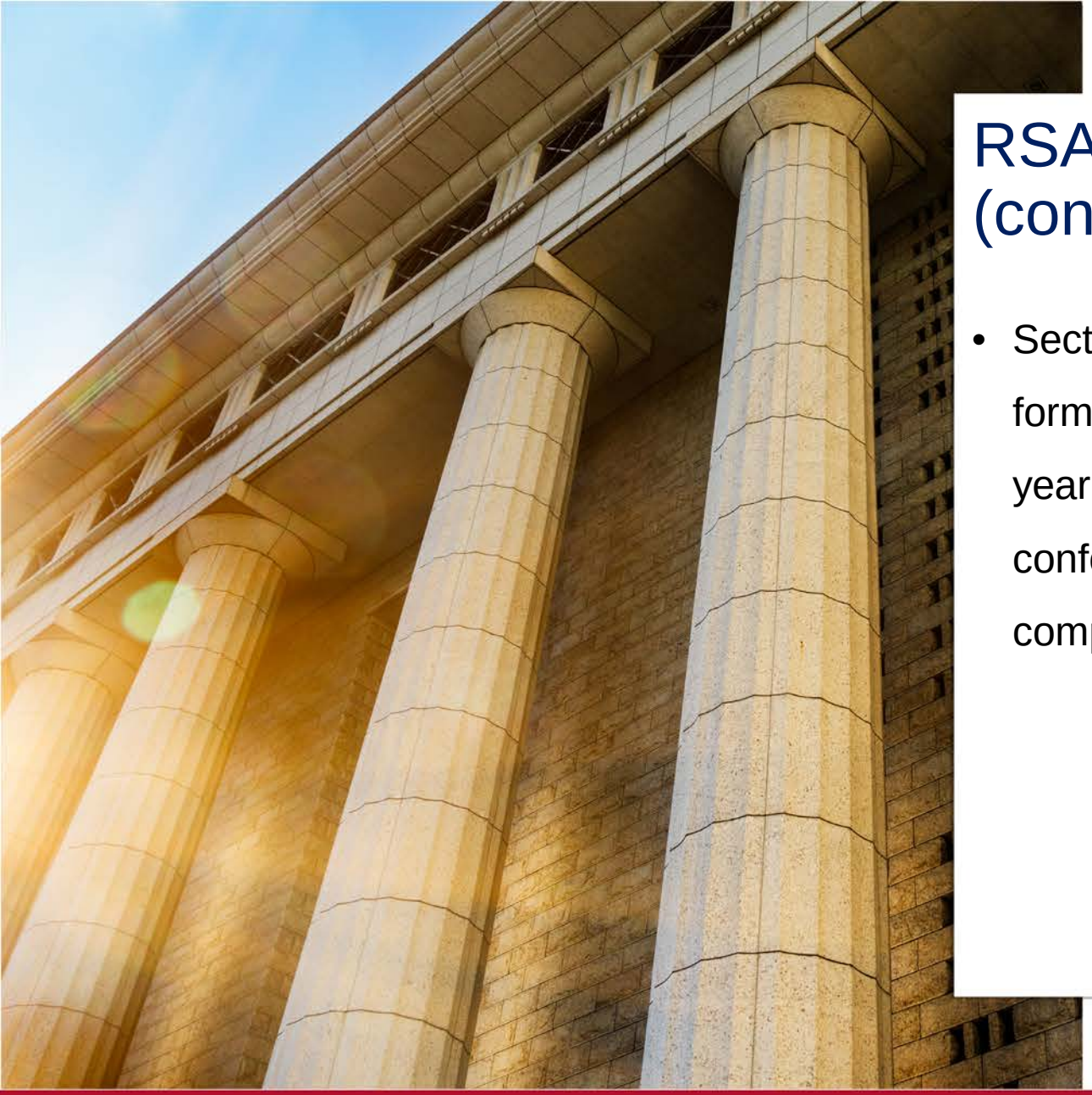
RSA FOLLOWING THE TREND (cont.)

- Much has since been done in that regard which culminated in the commencement of a number of remaining sections which has now been proclaimed by the President. The relevant sections and the applicable dates are as follows:-
- Sections 2a to 38; sections 55 to 109; section 111; and section 114(1), (2) and (3) commenced on 01 July 2020.
- Sections 110 and 114(4) shall commence on 30 June 2021.



RSA FOLLOWING THE TREND (cont.)

- The sections which commenced on 01 July 2020 are essential parts of the Act and comprise sections which pertain to, amongst others, the conditions for the lawful processing of personal information; the regulation of the processing of special personal information; Codes of Conduct issued by the Information Regulator; procedures for dealing with complaints; provisions regulating direct marketing by means of unsolicited electronic communication, and general enforcement of the Act.



RSA FOLLOWING THE TREND (cont.)

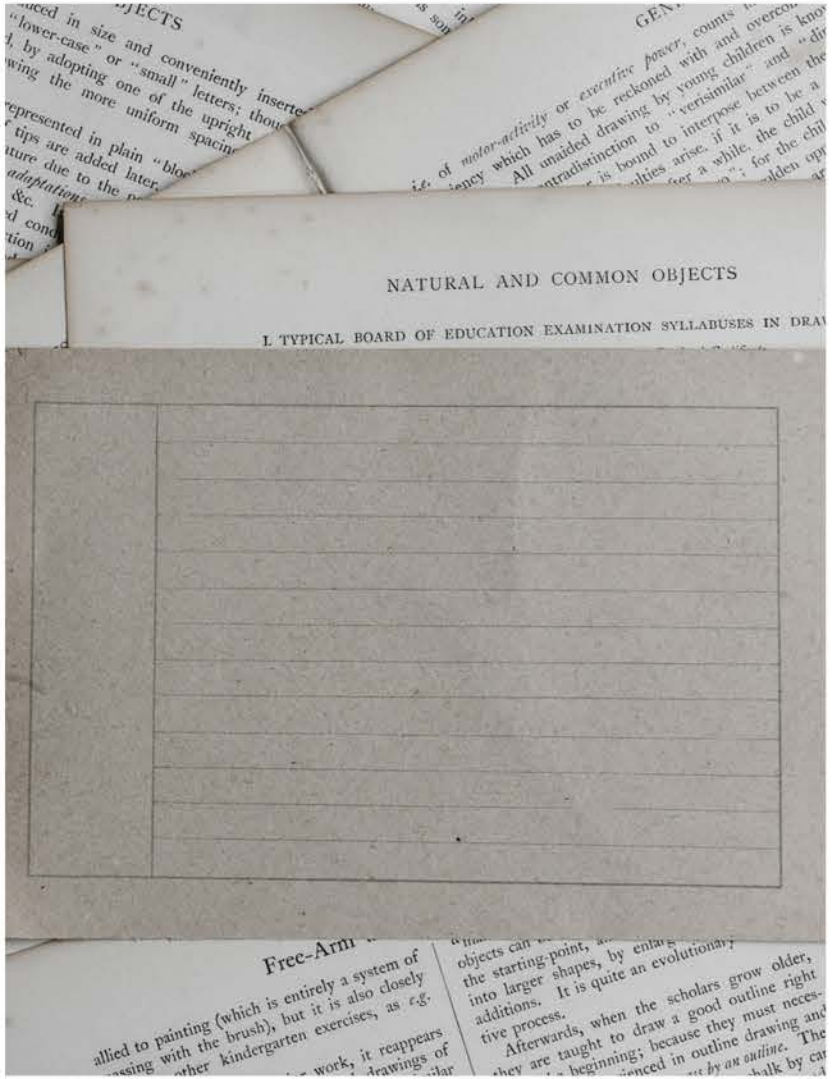
- Section 114(1) is of particular importance as it stipulates that all forms of processing of personal information must, within one year after the commencement of the section, be made to conform to the Act/ This means that entities must ensure compliance with the Act effective 01 July 2021.

SOME DEFINITIONS IN THE ACT

- Consent – means any voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to him or her.
- Data subject – means the person to whom personal information relates.
- Personal information – means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, juristic person, including but not limited to –

(1) Information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour sexual orientation, age, physical or mental health, well being, disability, religion, conscience, belief, culture, language and birth of person

(2) Information relating to the education or medical, financial, criminal or employment history of person



DEFINITIONS (cont.)

(3) Any identifying number, symbol, email address, physical address, telephone number or other particular assignment to the person;

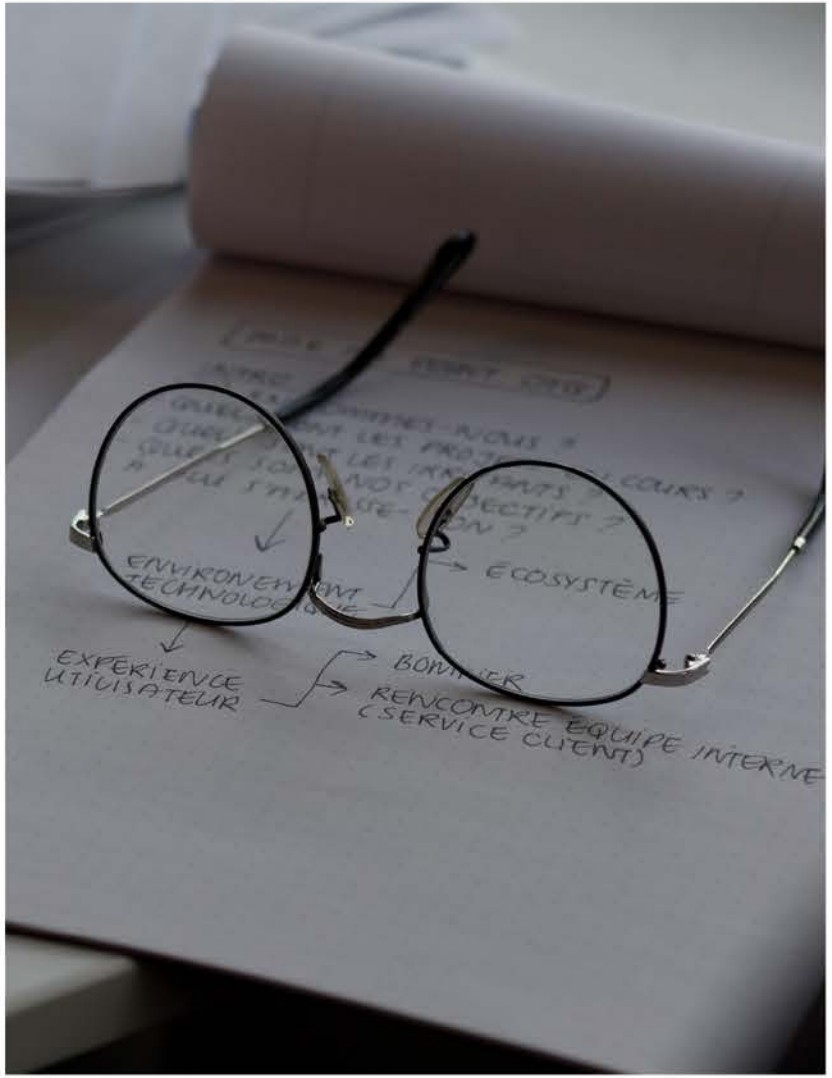
(4) The blood type or any other biometric information of the person;

(5) Personal opinions, views or preferences of the person;

(6) 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;

(7) The views or opinions of another individual about the person and

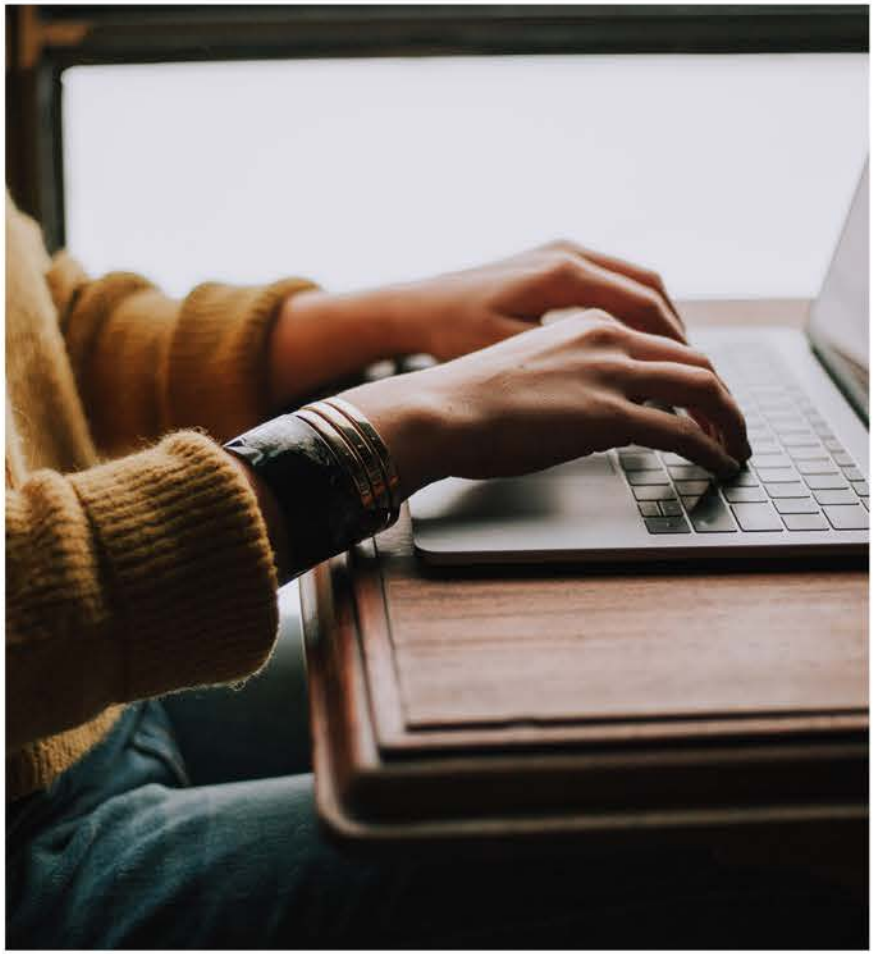
(8) The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.



DEFINITIONS (cont.)

- Responsible Party means a private or public body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information;

That is a person who processes information.



APPLICATION OF THE ACT

POPIA applies to the processing of personal information:-

- Entered in a record by or for a responsible party (i.e. UFS);
- Who is either domiciled in the RSA; or
- Which is not domiciled in the RSA,

using automated or nonautomated means situated in the RSA.

Clause 6 provides that the Act binds all

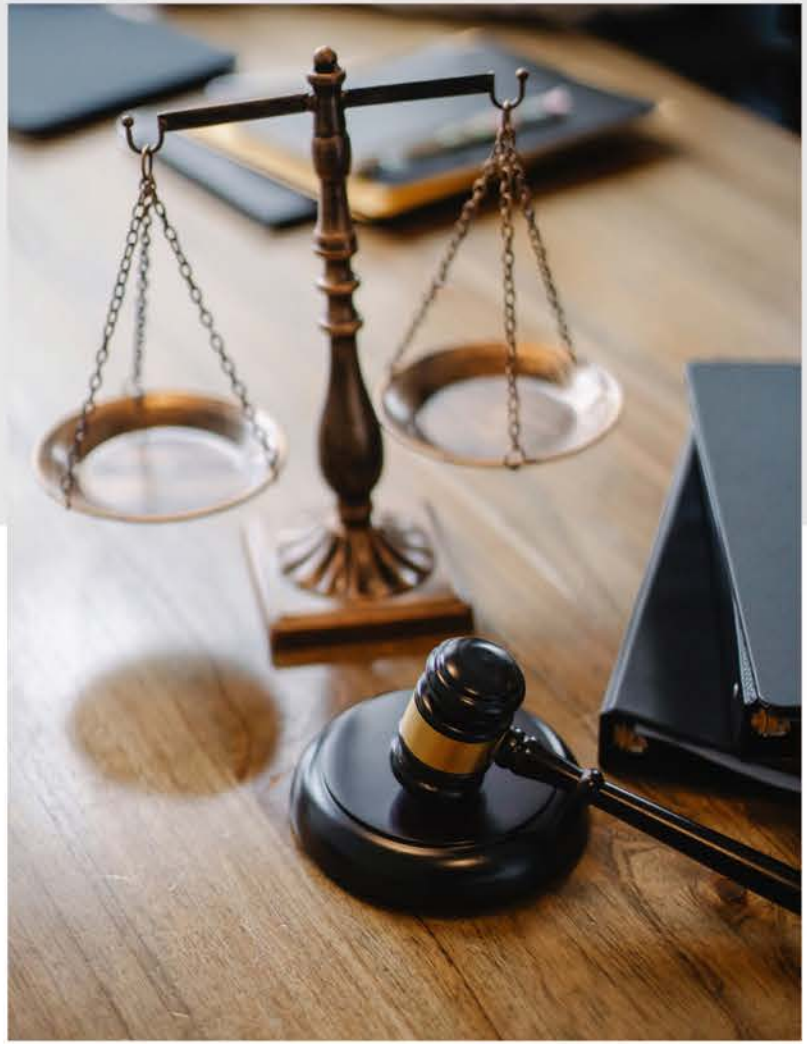
- Public and
- Private bodies

BINDS

EXCLUSIONS

The Act does not apply to:-

- de-identified information and
- processing done for purely household activities.



EXCLUSIONS: POLICE OR SAFETY AFFAIRS

- POPIA does not apply to the processing of personal information by or on behalf of the state and which involves national security, defence or public safety; or the purpose on which is the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information.

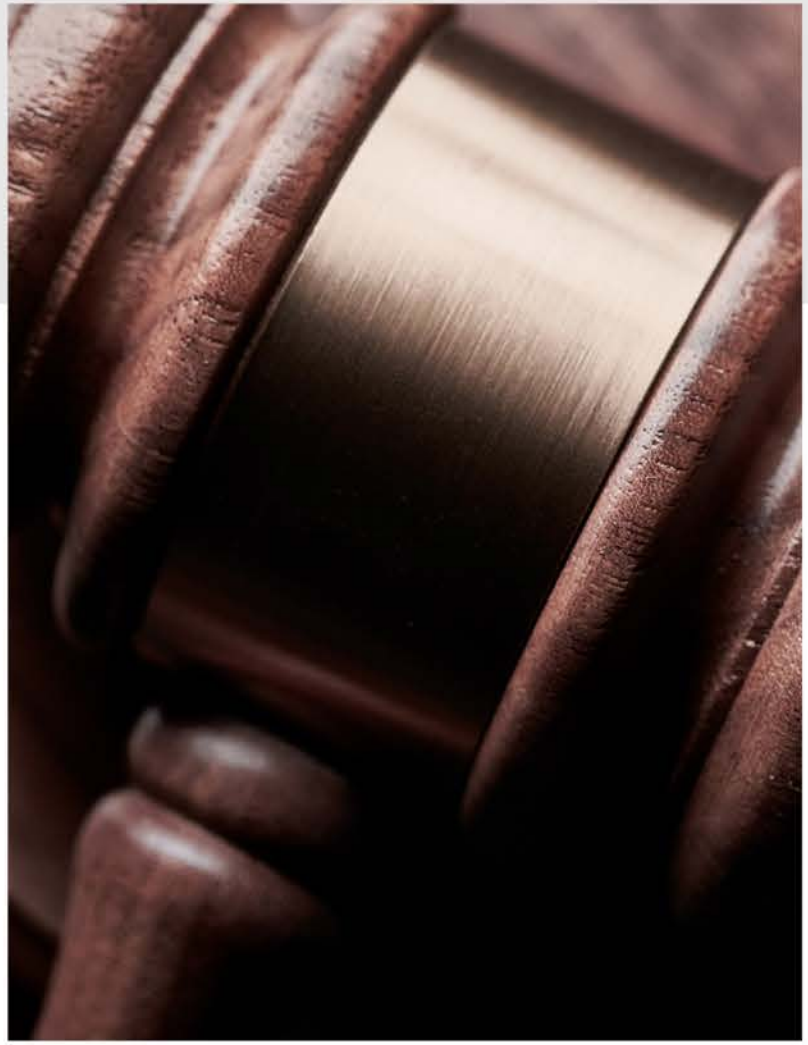
EXCLUSIONS - PRESS

- POPIA does not apply to the processing of personal information which is to be used for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession a code of ethics that provides adequate safeguards for the protection of personal information.

EXCLUSIONS POLITICIANS/COURTS

POPIA does not apply to the processing of personal information which is to be used

- by Cabinet and its committees, the Executive Council of a province and a Municipal Council of municipality;
- relating to the judicial functions of a court referred to in S66 of the Constitution; or
- that has been exempted from the application of the information protection principles in terms of S 34.



WHO DOES POPIA APPLY TO?

- Responsible Party (i.e. UFS)
- Private and Public Bodies who process information;
- Protects Data Subjects (employees, lecturers, students and third parties)
- Any person whose information is processed

Includes private individuals and trading entities too

TYPES OF INFORMATION

POPIA draws distinction between personal information and special personal information.

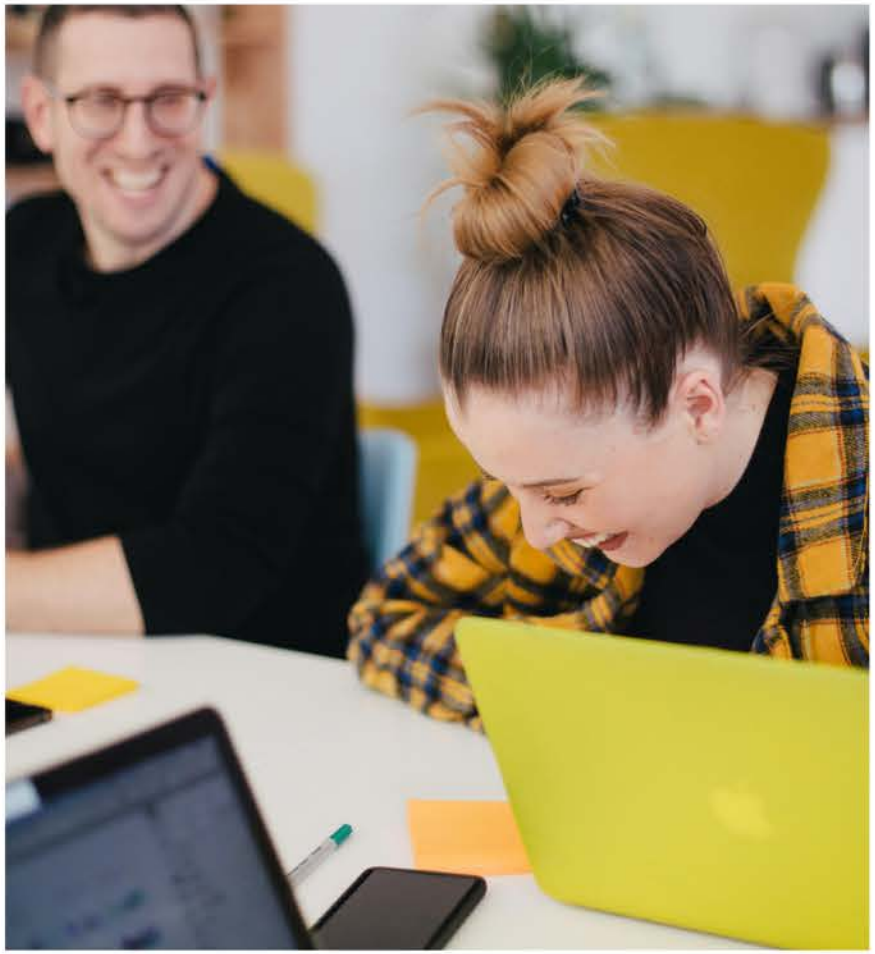
Special personal information – is defined in S 26 as information concerning:-

(1) a child, who is subject to parental control in terms of the law; or

(2) a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.

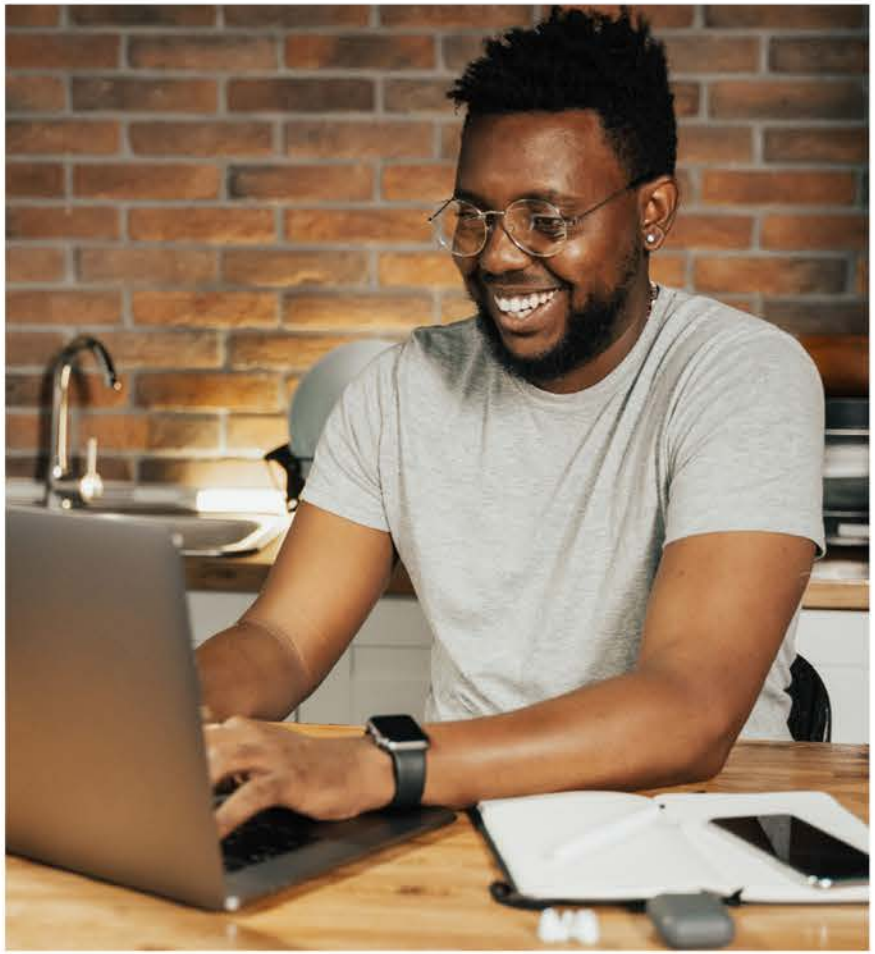
The Act places a prohibition on the processing of special personal information by responsible parties (i.e. private or public bodies).

But subject to a vast of personal exceptions.



EXAMPLES OF PERSONAL INFORMATION

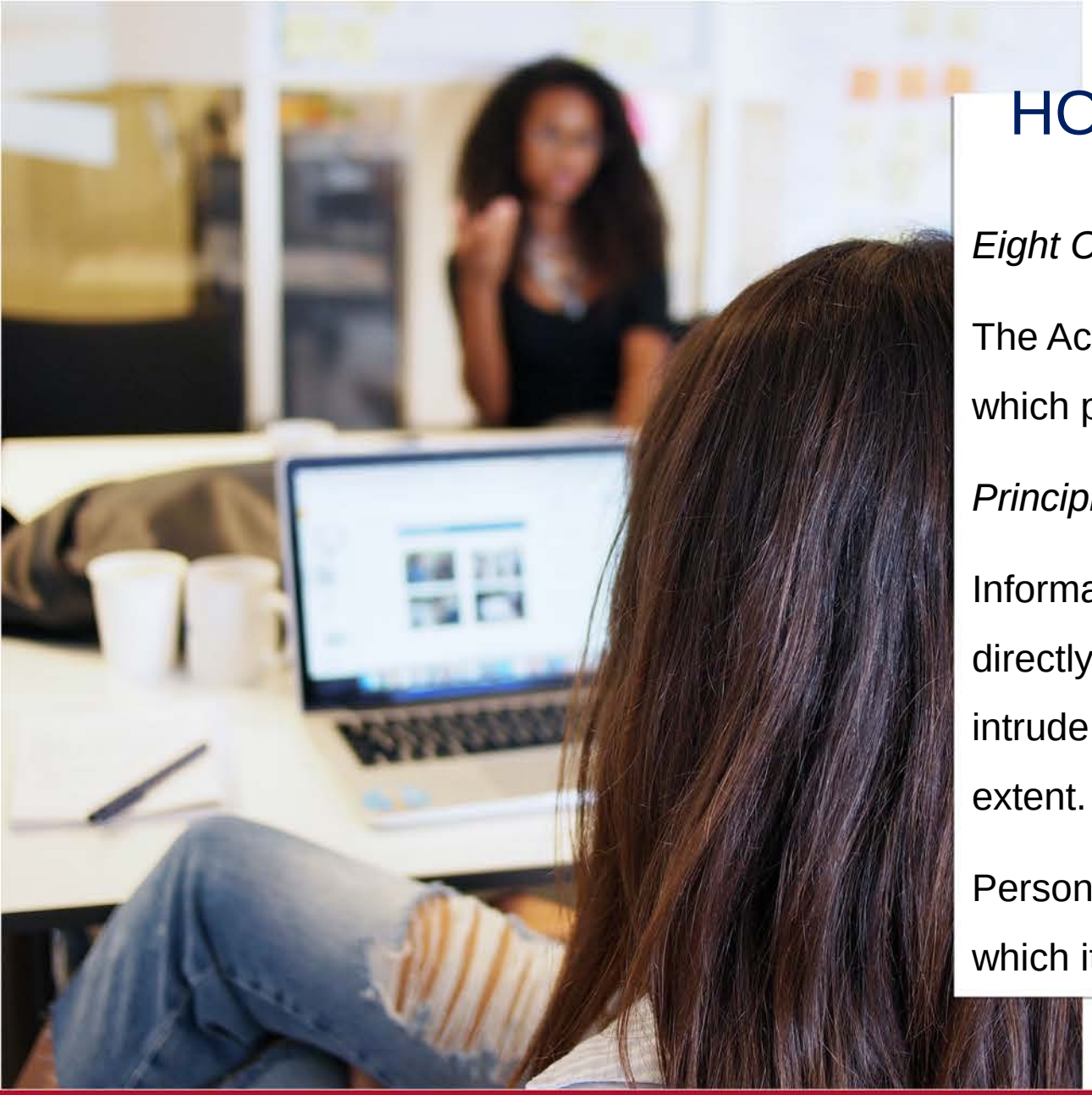
- Tenders
- General enquiries
- Vendor documents
- Client’s financials and details
- Client listings
- Contracts
- Transactional history
- Emails
- Queries



EXAMPLES OF PERSONAL INFORMATION (cont.)

HUMAN CAPITAL RECORDS/ HR

- Job applications
- Medicals – pre and post employment
- Qualifications
- Testimonials
- Employment history
- Health
- Criminal history



HOW MUST UFS TREAT & HANDLE THIS INFO

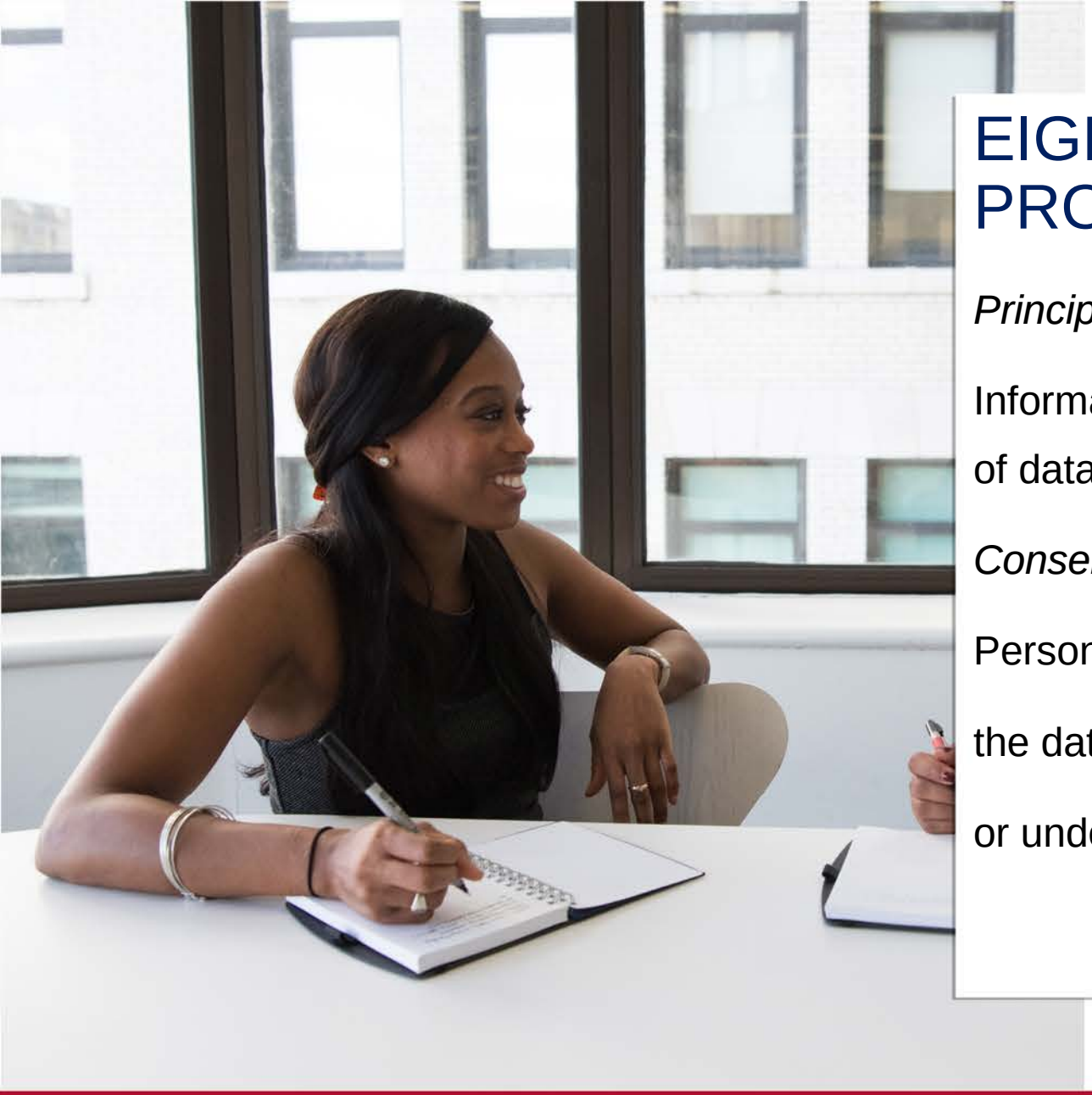
Eight Core Information Protection Principles

The Act gives effect to eight core information protection principles which prescribe how personal information is to be processed.

Principle One – Necessary

Information can only be collected or stored if it is necessary for or directly related to a lawful, explicitly defined purpose and does not intrude upon the privacy of the data subject to an unreasonable extent.

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.



EIGHT CORE INFORMATION PROTECTION PRINCIPLES (cont.)

Principle Two – Consent

Information must be collected directly from and with the consent of data subject

Consent and Justification

Personal information may only be processed if –

the data subject consents to the processing;

or under the following circumstances:

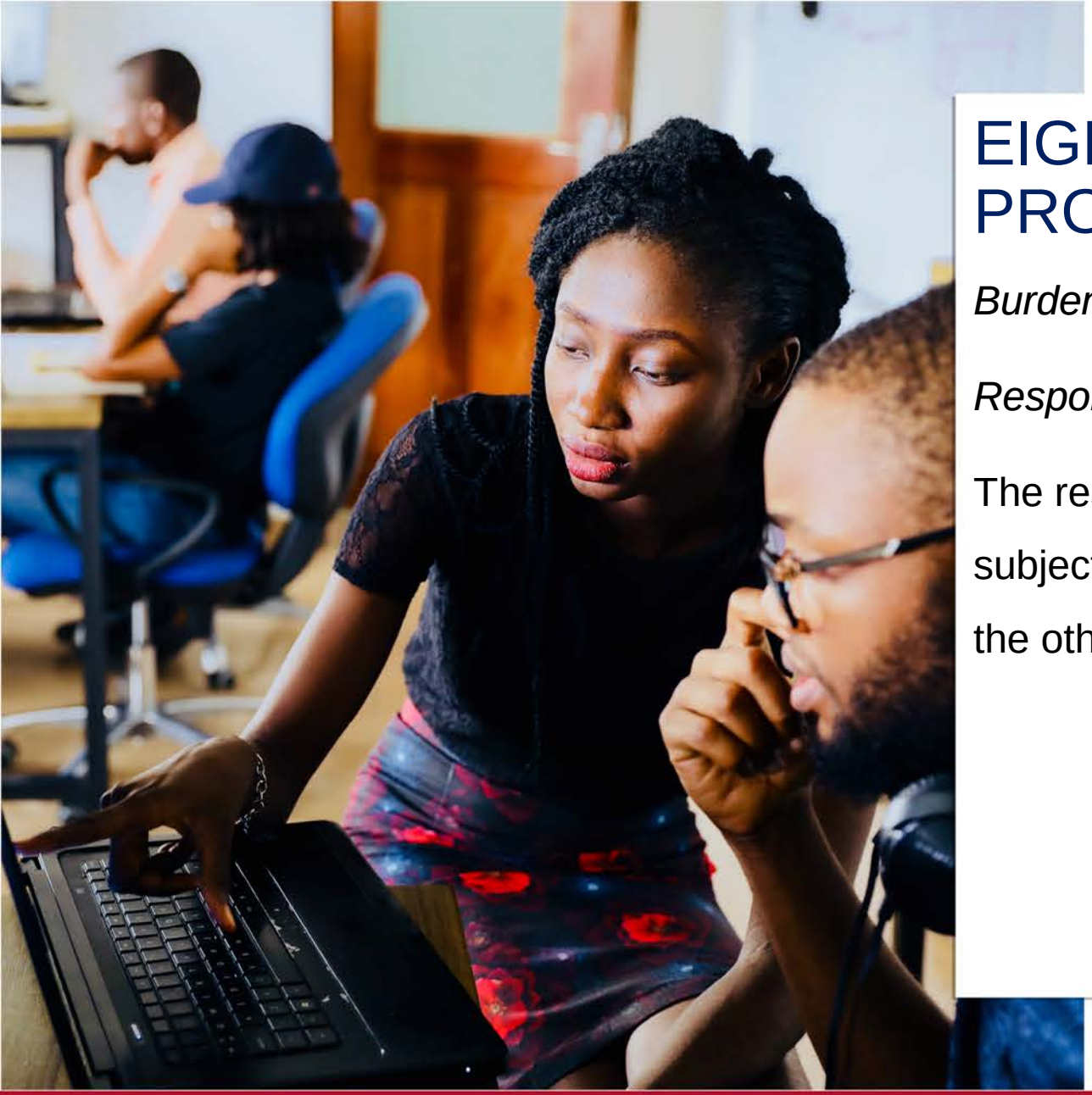
- S 11 & 12

EIGHT CORE INFORMATION PROTECTION PRINCIPLES (cont.)

Justification

If-

- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party (i.e. employment contract);
- processing complies with an obligation imposed by law on the responsible party (for e.g. BCEA, UIF, etc)
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a 3rd party to whom the info is supplied



EIGHT CORE INFORMATION PROTECTION PRINCIPLES (cont.)

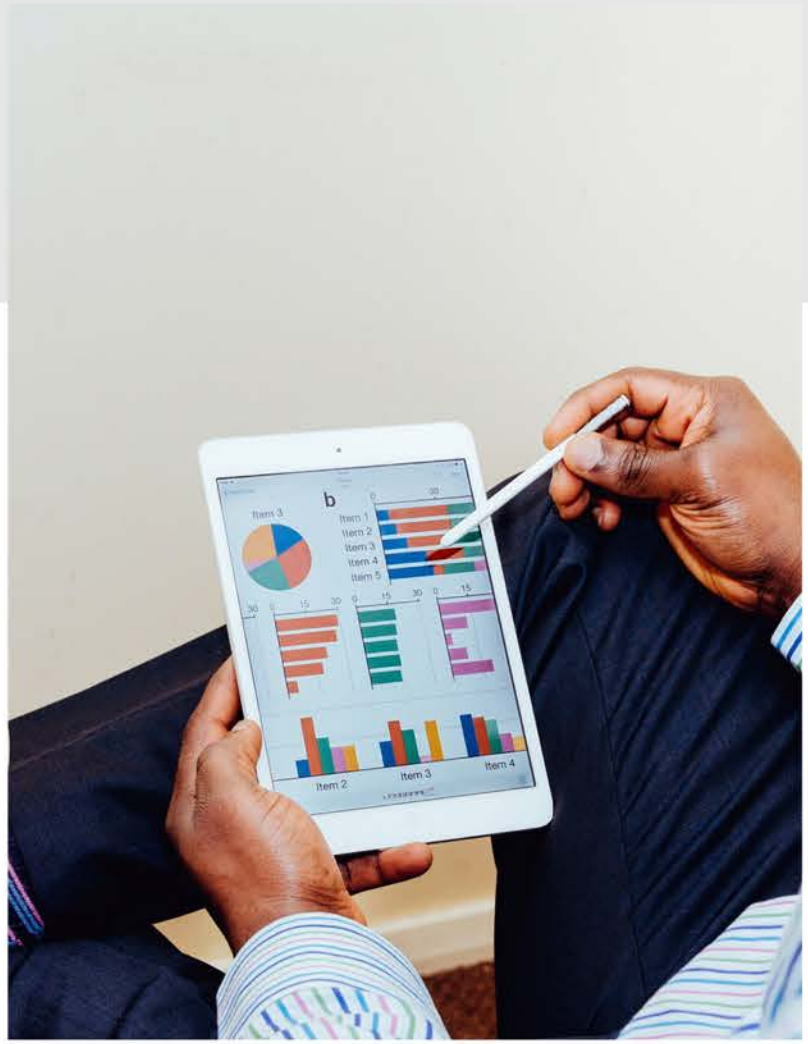
Burden of Proof

Responsible party to obtain consent

The responsible party must prove that it has obtained the data subject's consent, or must provide reasons why it had to rely on the other provisions where consent is not obtained.

WITHDRAWAL

- The data subject or competent person may withdraw his, her or its consent at any time to the processing.
- NB: the lawfulness of the processing of personal information before such withdrawal or objection will not be affected.



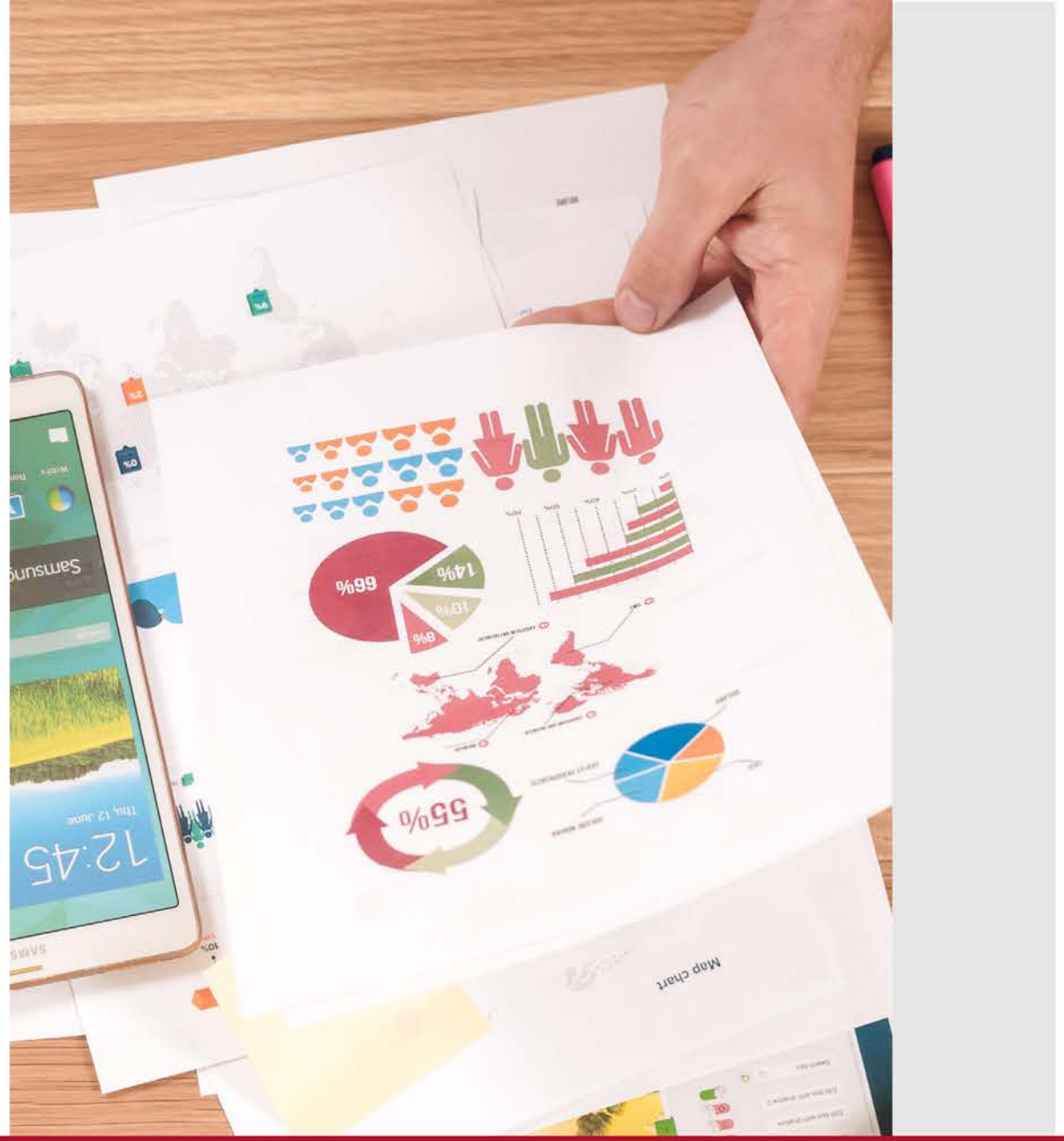
COLLECTION DIRECTLY FROM DATA SUBJECT

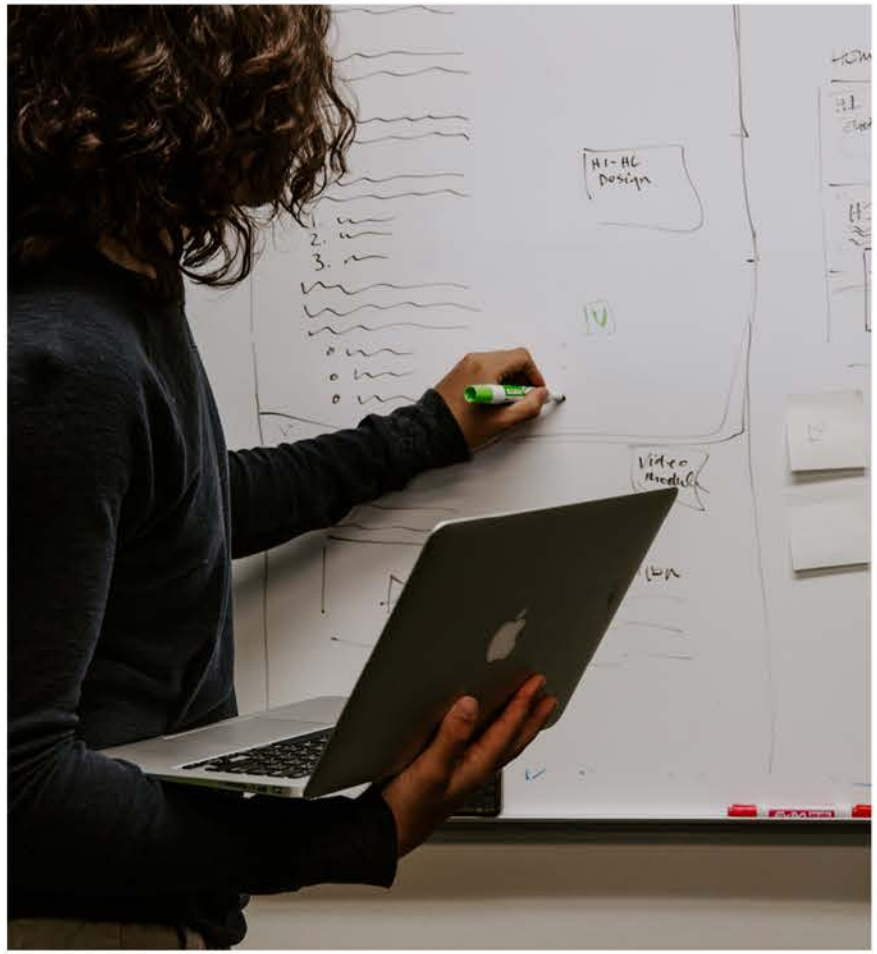
- Personal information must be collected directly from the data subject,

except as otherwise provided….

i.e. when applying for the position or an account

- S11 & S12.





PRINCIPLE 3 - INFORMED

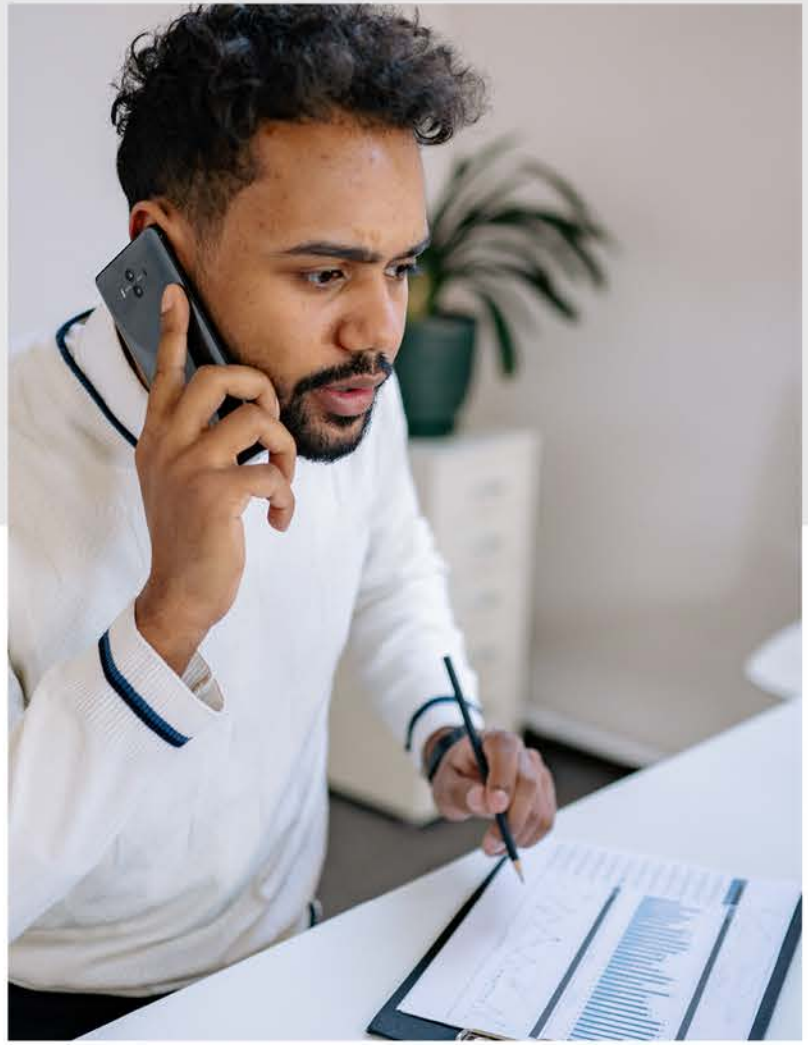
- Data subjects must be informed of the purpose of any such collection and of the intended recipients of the information, at the time of collection.

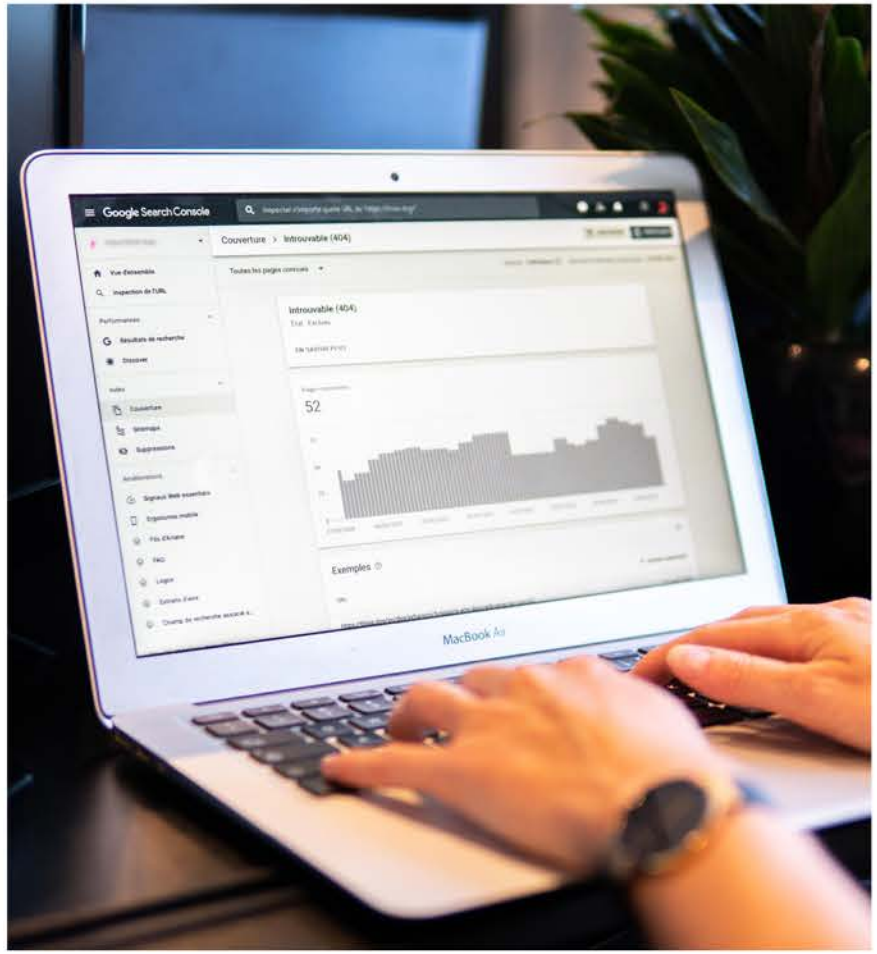
COLLECTION FOR SPECIFIC PURPOSE

S13. Collection for specific purpose

- Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party and the data subject must be made aware of the purpose.

- S13 & S18.





NB

Steps must be taken in accordance with section 18 to ensure that the data subject is aware of the purpose of the collection of the information.

- S18.

DATA SUBJECT AWARE OF PURPOSE

SECTION 18 STATES

If personal information is collected, the responsible party must take

reasonably practicable steps to ensure that the data subject is aware of —

- the information being collected;
- the name and address of the responsible party;
- the purpose for which the information is being collected;
- whether or not the supply of the information by that data subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- any particular law (i.e. labour laws) authorising or requiring the collection of the information;
- whether the data is to be transferred to another country and the security measures in place to protect any invasions of privacy in that country ….

SECTION 18 (cont.)

And….. any further information, such as the—

- recipient or category of recipients of the information;
- nature or category of the information; and
- existence of the right of access to and the right to rectify the information collected, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

NB: It is not necessary for a responsible party to comply with these notification requirements if noncompliance would not prejudice the legitimate interests of the Data subject or Responsible party as set out in terms of this Act.

(Disclosure details)

STEPS

The steps must be taken—

- in respect of direct collection from the data subject: before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or
- in any other case: before the information is collected or as soon as reasonably practicable after it has been collected.

WHAT DO YOU DO WITH THE DATA

- Principle 4 – Not distributed

Information must not be distributed in a way incompatible with the purpose for which is was collected.

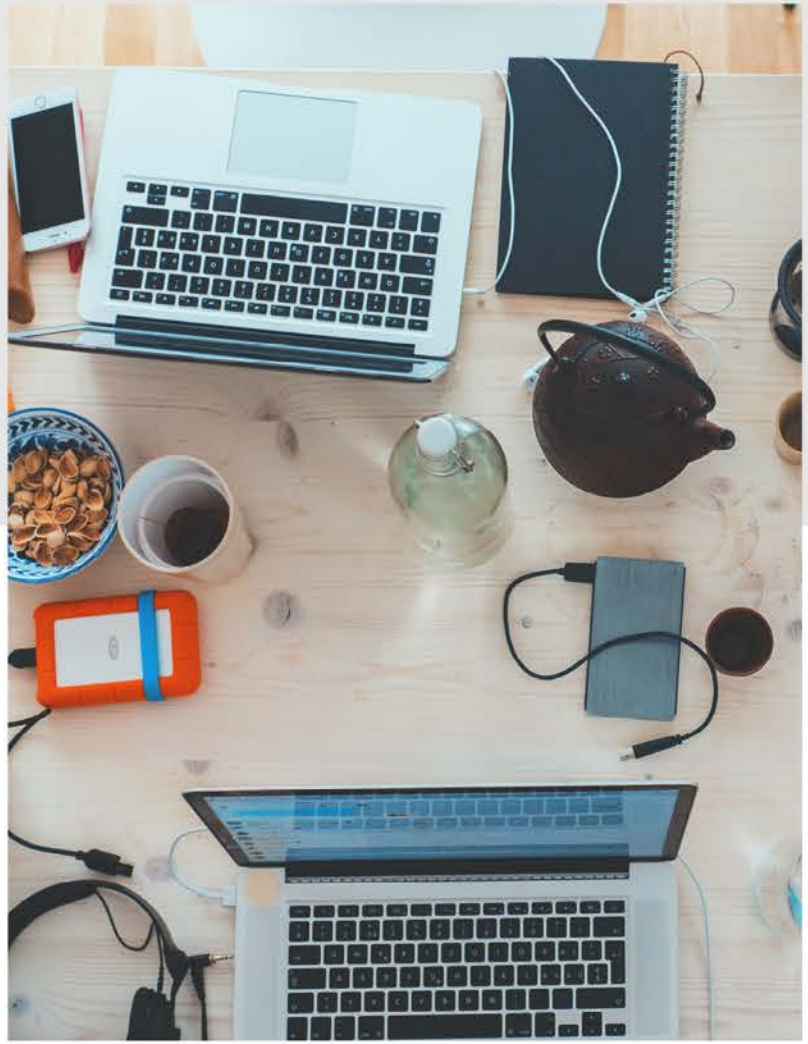
- Principle 5 – Updated

Reasonable steps must be taken to ensure that the information processed is accurate, up to date and complete.

COMPLETE AND ACCURATE AND UP-TO-DATE

- The responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.
- In taking these steps the responsible party must have regard to the purpose for which personal information is collected or further processed.

- S 16.



PRINCIPLE 6 – SAFEGUARDED

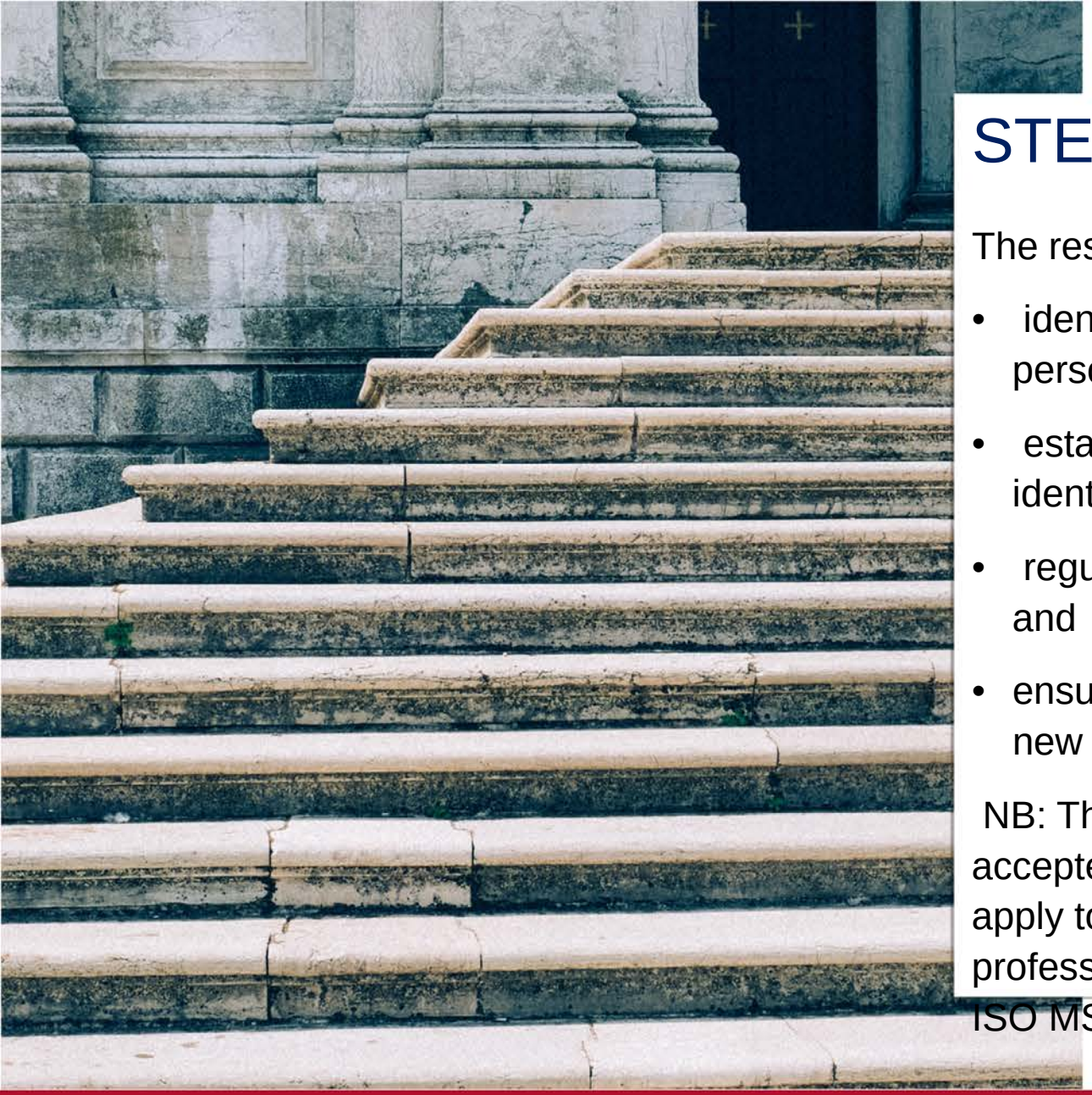
Appropriate technical and organisational measures have to be taken to safeguard the data subject against the risk of loss, damage, destruction of or unauthorised access to personal information.

SECURITY MEASURES ON INTEGRITY OF PERSONAL INFORMATION

A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

- loss of, damage to or unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.

- s19.



STEPS TO SECURE

The responsible party must take reasonable measures to—

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

NB: The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations; for example any SANS Code or ISO MS

What about your contractors - where housing and processing of information is done by an outside service provider?

OUTSOURCING

OPERATORS

An operator or anyone processing personal information on behalf of a responsible party or an operator, must—

- process such information only with the knowledge or authorisation of the responsible party; and
- treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

- S20.

SECURITY MEASURES

A responsible party must ensure that an operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

- S 21.

WRITTEN CONTRACT

The processing of personal information for a responsible party by an operator on behalf of the responsible party must be governed by a written contract between the operator and the responsible party, which requires the operator to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

OUTSIDE RSA

If the operator is not domiciled in the Republic, the responsible party must take reasonably practicable steps to ensure that the operator complies with the laws, if any, relating to the protection of personal information of the territory in which the operator is domiciled.

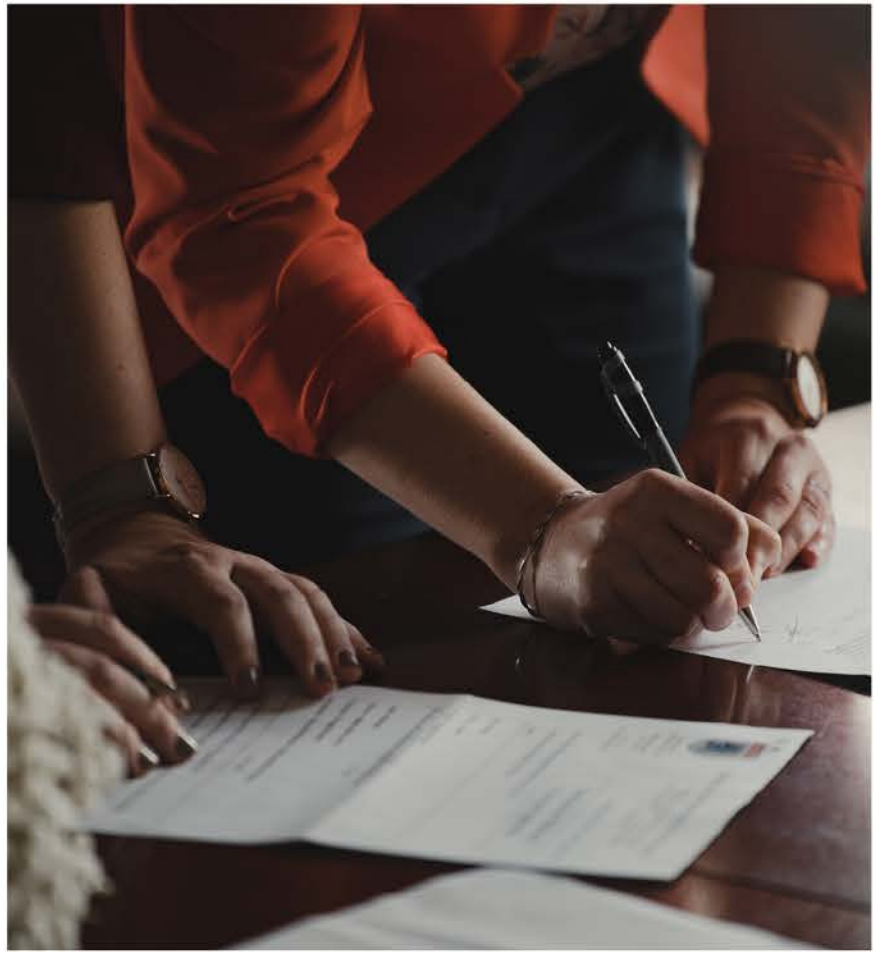
Notification of security compromises

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party, or any third party processing personal information under the authority of a responsible party, must notify the—

- Regulator; and
- data subject, unless the identity of such data subject can not be established.

- S 22.

WHAT HAPPENS IF SECURITY IS COMPROMISED



Data subjects are allowed a right of access to their personal information and a right to demand correction if such information should turn out to be inaccurate.

PRINCIPLE 7 - ACCESS

ACCESS TO PERSONAL INFORMATION

A data subject, having provided adequate proof of identity, has the right to—

- request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

BUT MUST do so by using the PAIA process.

- S23.

RETENTION OF RECORDS

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

- S14.

- retention of the record is required or authorised by law;
- the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
- retention of the record is required by a contract between the parties thereto; or
- the data subject has consented to the retention of the record.

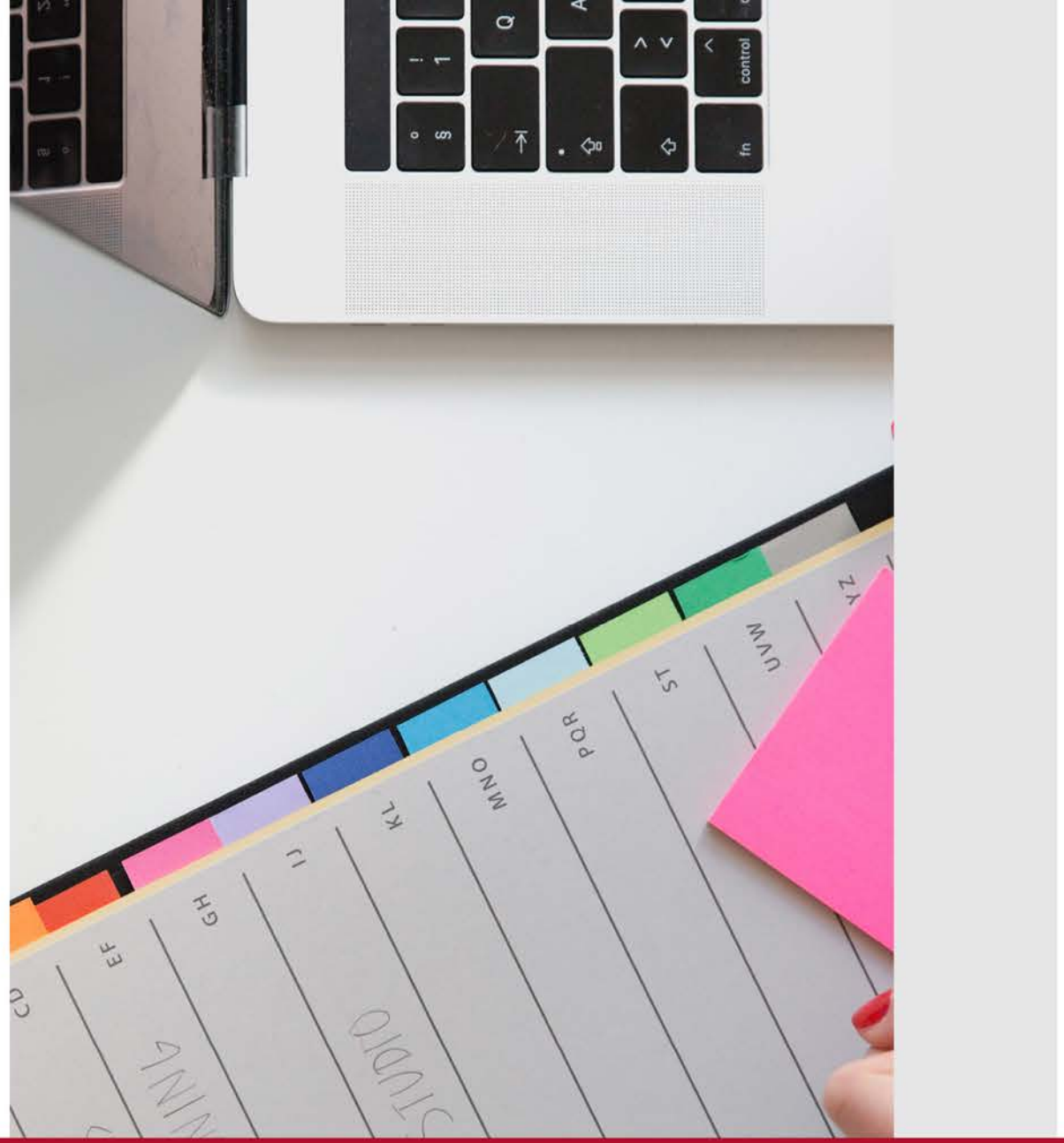
EXCESSIVE RETENTION PERIODS

Records of personal information may be retained for periods in excess of those contemplated above for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

RETENTION PERIODS

A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, (i.e. job application) must—

- retain the record for such period as may be required or prescribed by law or a code of conduct; or
- 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.



Destroy

- 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.
- The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

WHAT DO YOU DO WITH INFORMATION AFTER USAGE

IMPACT ON UFS STAFF

NB

- Processing must be in line with the POPI Act, the 8 core Information Protection Principles, and any other applicable laws.

REGULATOR, EC AND INFO OFFICERS

The Regulator will ensure that POPI is complied with.

The Regulator must establish an Enforcement Committee who will assist with this task.

A Company’s Information Officer will be responsible for ensuring that it and its employees comply with POPI.

REGISTRATION

Information Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Registrar.

COMPLAINTS

Any person may submit a complaint to the Regulator in the prescribed manner and form—

- alleging interference with the protection of the personal information of a data subject; or
- if the data subject is aggrieved by the determination of an adjudicator.

- S.74

ADMINISTARTIVE FINES

If a responsible party is alleged to have committed an offence in terms of this Act, it could be penalised by way of an administrative fine, which amount may, not exceed R10 million.

A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act, whether or not there is intent or negligence on the part of the responsible party.

- S.99

CIVIL REMEDIES

PENAL SANCTIONS

Any person convicted of an offence in terms of this Act, is liable, in the case of a contravention of—

- section 100, 103(1), 104(2), 105(1), 106(1), (3) or (4) to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment; or
- 100-OBSTRUCTION OF REGULATOR.
- 104-OFFENCES BY WITNESSES.
- 105-UNLAWFUL ACTS BY RESPONSIBLE PARTY IN CONNECTION WITH ACCOUNT NUMBER.
- 106-UNLAWFUL ACTS BY THIRD PARTIES IN CONNECTION WITH ACCOUNT NUMBER.

PENAL SANCTIONS (CONT.)

Any person convicted of an offence in terms of this Act, is liable, in the case of a contravention of—

- section 59, 101, 102, 103(2) or 104(1), to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment
- 059-FAILURE TO NOTIFY PROCESSING SUBJECT TO PRIOR AUTHORISATION.
- 101-BREACH OF CONFIDENTIALITY.
- 102-OBSTRUCTION OF EXECUTION OF WARRANT.
- 103-FAILURE TO COMPLY WITH ENFORCEMENT OR INFORMATION
- 104-OFFENCES BY WITNESSES.

THANK YOU

Comments	Questions	Answers