UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

1922 2022

North West University

What are the Implications of POPIA on the Research Environment?

Protection of Personal Information Act No. 4 of 2013 (POPIA) and

the Academy of Science of South Africa (Assaf)

***Working Draft* Code of Conduct for Research**

Eleni Flack-Davison

University of the Witwatersrand, Johannesburg

Legal Adviser (Admitted Attorney of the High Court of South Africa)

Research Compliance Manager

Head: Research Integrity Office

Research Data Protection Officer

Email: eleni.flack-davison@wits.ac.za

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Aim of the Session:

To understand:

1. Broad application of the POPI Act
2. Application process for the Code of Conduct regarding the processing of personal information of identifiable research participants for research in South Africa
3. Who is responsible for ensuring that the research complies with the code

Right to Privacy – Personal Information

- POPIA regulates the processing of personal information in South Africa
- Personal information is a sub-right of the right to privacy, found in s14 of the South African Constitution:
- Privacy:
  - 14. Everyone has the right to privacy, which includes the right not to have—
  - (a)their person or home searched;
  - (b) their property searched;
  - (c) their possessions seized; or
  - (d) the privacy of their communications infringed.
- Privacy is not an absolute right and may be subject to justifiable limitations.

PoPIA – Broad Application

POPIA applies to:

- Processing of personal information by public and private entities domiciled in South Africa or where information processing (whether automatic or not) takes place within South Africa.
- POPIA does not apply to the processing of personal information:
  - that has been de-identified: such information must be in a state that it can no longer be re-identified
  - Information processed for purely household use

What is Personal Information?

- A record of any kind containing information that can – though a reasonably foreseeable method – be used to identify an individual.
  - Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to information relating to —

Name/ID no.

Race/Gender/Sexual Orientation

Pregnancy

Marital Status

Physical/ Mental Health

Age

National/Ethnic/ Social Origin

Disability

Religion/ Beliefs /Culture

Language

Email Address/ Contact Numbers

Location/ Physical Address

Educational/Medical /Financial/ Criminal or Employment History

Photos/Video Footage
Voice Recordings/Biometrics

Personal Opinion, View, Preferences

What is de-identified information?

- De-identified information is information which cannot be linked, through any foreseeable method to an individual
- **De-identify information**, in relation to personal information of a Data Subject, means to delete any information that—
    - identifies the Data Subject;
    - can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
    - can be linked by a reasonably foreseeable method to other information that identifies the data subject, and 'de-identified' has a corresponding meaning.

Role Players – POPIA Definitions

- **Person:** A natural or juristic person
- **Data Subject:** Person to whom the personal information relates to and partakes in the research **(e.g. Research Participant)**
- **Responsible Party:** A public body or private body or any other person which, alone or in conjunction with others, determines the purpose and means for processing personal information, and is responsible for the lawful processing of such information

(e.g. University for everyday compliance, Researcher for research being done)

- **Operator:** A Person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the authority of that party

(e.g. translator, community liaison, scribe)

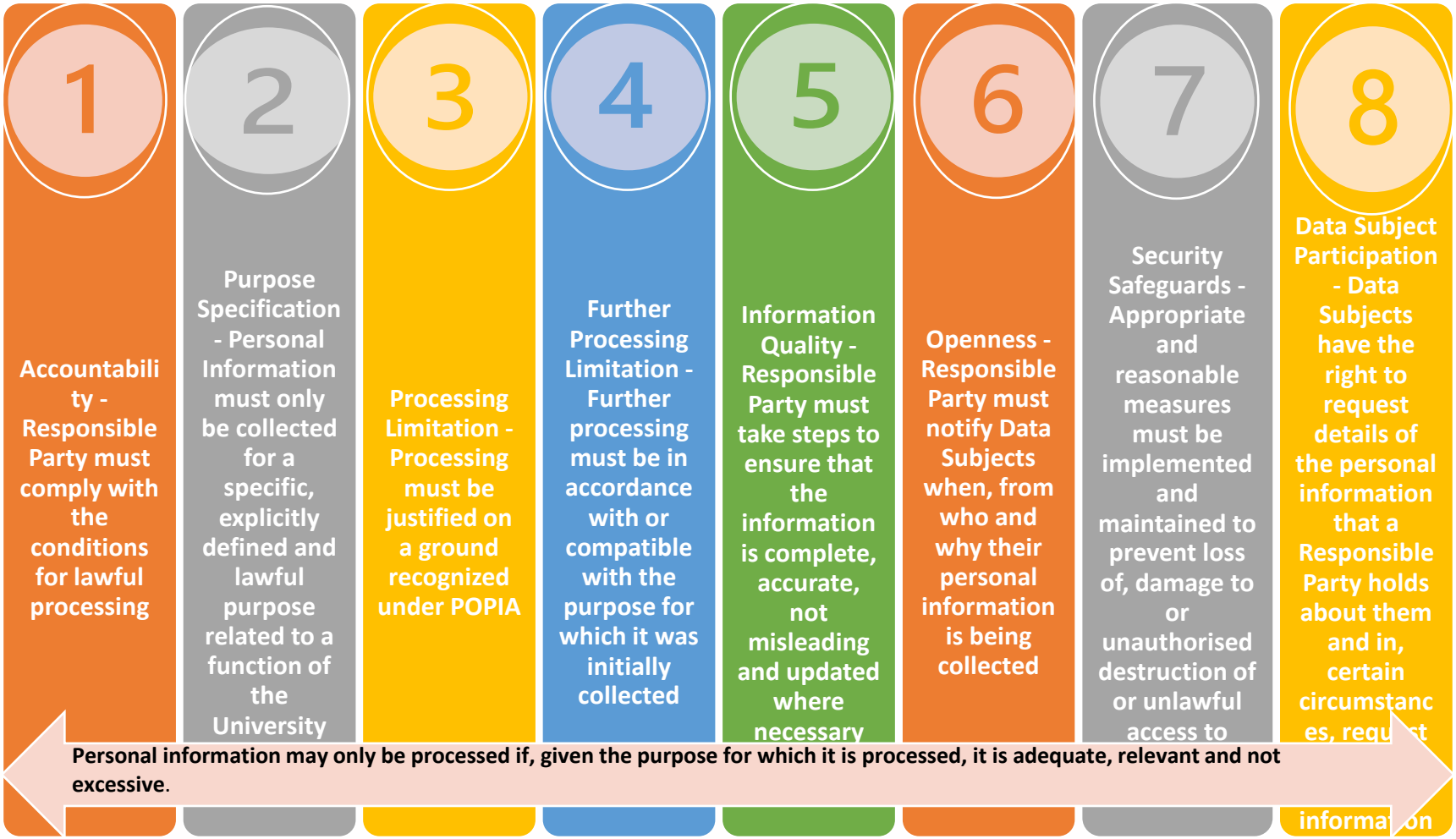
- **Information Officer:** An official in the employ of the Responsible Party who is responsible for the receipt of requests for information

Rights of Data Subject

- Notified by the Responsible Party of the processing of his/her Personal Information
- To know what personal information is being held and to request access, correction, destruction or deletion of this Personal Information
- To object on reasonable grounds to the processing of his / her Personal Information including for direct marketing purposes
- To submit a complaint to the Information Regulator and to institute civil proceedings if aggrieved

8 Conditions for Lawful Processing

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG



Lawful Conditions for Processing of Personal Information

1. Accountability:

- Responsible Party must ensure that all the conditions laid out in the POPIA are complied with at the time of the determination of the purpose of processing and during processing itself.

2. **Processing Limitations:**

- There must be a lawful basis to process Personal Information
- Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive;
- Consent, justification and objection: Personal Information can only be processed if it is necessary for performance of a contract, obliged by law, for a legitimate interest, or for the performance of a public law duty;
- Collection from the Data Subject: except where the Personal Information is already contained in a public record, or where it would maintain the legitimate interest of the Data Subject, Responsible Party of third party, or where it is for research purposes and reasonably impractical.

Lawful Conditions for Processing of Personal Information

3. **Purpose Specification**

- Information must be collected for a specific purpose ("specific, explicitly defined and lawful") and not used for any other purpose besides this.
- Records containing Personal Information must not be retained longer than necessary to fulfil the original purpose unless:
  - required by law;
  - retention of the record is required by an agreement with a third party;
  - the consent of the Data Subject is given.
  - required for research purposes and safeguards are in place
  - Records containing personal information can be destroyed, deleted or de-identified.

Lawful Conditions for Processing of Personal Information

4. **Further Processing**
    - Further processing to be compatible with the original purpose i.e. research
    - In determining this the responsible party must:
        - Look at relationship between new purpose and original purpose;
        - Nature of information;
        - Consequences;
        - Manner of collection;
        - Contractual rights and obligations.
- It is valid if:
    - If one is further processing for research purposes, and there are safeguards in place to ensure that the information will not be used for any other purpose and not published in an identifiable form.
    - The consent of the Data Subject is given;
    - The information is already in the public domain;
    - For reasons of public interest (e.g. World Pandemic)

Lawful Conditions for Processing of Personal Information

5. **Information Quality**

- Responsible Party must ensure the quality of the information that is kept and stored.
- "Quality" refers to information that is complete, accurate, not misleading and updated.
- In ensuring information quality, the Responsible Party must comply with the original purpose of the collection of information
- Annual audits to check information quality

Lawful Conditions for Processing of Personal Information

6. **<u>Openness / Transparency</u>**

- Maintain documentation for record keeping purposes of all personal information processing operations.
- Notification to Data Subject when collecting Personal Information. The Data subject must be made aware of:
  - Where his/her data was collected from;
  - The contact details of the Responsible Party;
  - The purpose for which the information was collected;
  - Where applicable, that the Responsible Party intends on transferring the information to a third country and the level of Personal Information protection offered.
- Responsible Party is exempt from notification to the Data Subject if:
  - If the Data Subject has already given consent for non-compliance with notification;
  - Compliance is not “reasonably practicable”
  - If the information is de-identified or used for statistical, historical or research purposes.

Lawful Conditions for Processing of Personal Information

7. **Security Safeguards**

- Security measures to ensure the integrity and confidentiality of Personal Information and its processing, including verifying the operator and persons acting under authority and their processes
- Security of the safekeeping – e.g. Password-protection, encrypted, using ReDCaPP
- E.g. of how not to keep data collected safe e.g. keep data collected on a hard drive in an unsecured place
- Notification of security compromises to IR and data subject

Lawful Conditions for Processing of Personal Information

8. **Data Subject Participation**

- Data Subjects have the right to request details of the personal information that a Responsible Party holds about them and in, certain circumstances, request access to such information
- Access to Personal Information (Promotion of Access to Information Act / PAIA)
- Correction of Personal Information
- Manner of access (Promotion of Access to Information Act / PAIA)

Authorisations for Processing Special Personal Information

Section 26 of POPIA - Prohibition on processing of special personal information

Special Personal Information is Information relating to:

- religious or philosophical beliefs;
- race or ethnic origin;
- trade union membership;
- political persuasion;
- health or sex life;
- biometric information;
- criminal behaviour of data subject.

- The same conditions and authorisations exist under POPIA for Personal Information relating to children.

Authorisations for Special Personal Information or Personal Information of Children

- Data Subject consent to the processing, Parental informed consent is required i.t.o. NHA or the competent person in the case of information relating to a child;
- NHA read in relation to the Children's Act;
- Children are seen as a part of a vulnerable group;
- Necessary for the establishment, exercise or defence of a right or obligation in law;
- Compliance with international public law;
- Been made public by the Data Subject;
- Or: for historical, statistical or research purposes to the extent that:
- the purpose serves a public interest and the processing is necessary for the purpose concerned; or
- it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent.

International Data Transfers

- POPIA - Section 72
- Authorised where:
- There is consent from the Data Subject
- The processing is necessary for the fulfilment of a law or contract
- Where there is a written agreement in place upholding the conditions of POPIA in the transfer (e.g. DTA)
- High risk transfers, requiring Prior Authorisation from the IR:
- Transferring Special Personal Information or Personal Information of a child to a foreign country without an adequate data protection law in place.

Comparison Table: Worldwide Data Privacy Regulations

	GDPR	CCPA	LGPD	POPI
Territorial Scope	Global	Statewide and global	Global	Restricted to organizations that are either based or process personal data in South Africa
Mandatory DSAR response times	Generally within a month	45-day window, with extensions of up to 90 days permitted.	Within 15 days	Within a reasonable time period
DPO	Mandatory for public-sector bodies and companies that process personal data at scale	None	Mandatory	Mandatory role known as Information Officer
Breach reporting deadlines	Within 72 hours	None, but other state laws require 72-hour deadlines	Within a reasonable time period	As soon as reasonably possible
Breach reporting deadlines	4% of global annual revenue or €20 million, depending on which is higher	$7500 per individual violation and personal claims of $750 per incident	2% of a company's Brazilian annual revenue, capped at R$50 million	R10 million fine or 10 years' imprisonment

Worldwide Data Privacy Regulations Compared

Searching for relevance: Comparing African data protection legislation just got easier

datalaw February 24, 2023 12:53 pm

The DS-I Africa Law group has developed a search tool to help you compare the most relevant areas of data protection legislation that impact your health research project.

DS-I Africa Law has launched a new data protection legislation search and compare tool. The tool allows researchers to quickly compare the data protection legislation of 12 African countries in which the DS-I Africa Law group conducts research.

The first version of the search tool is live on the DS-I Africa Law website and is free to use. Improvements and additions will be made over the year based on the needs of the DS-I Africa consortium, so continue to watch this space for exciting developments.

Click here

Data Transfers / Data Sharing Agreements

- Data Provider / Data Recipient
- Origins of the Data (i.e. jurisdiction, applicable law)
- What data is being transferred / shared?
- What can the data be used for / restrictions of use (i.e. no further transfer)
- How will the results be used / ownership?
- Ownership of the data
- Publication – Data, Results
- Access to the data
- Duration to have access and use of data
- Data Protection – compliance with legislation, process personal info for specific purpose, do not disclose to third parties (e.g. POPIA / GDPR)
- Security Safeguards in place
- How will confidential information be handled?
- *Due Diligence
- *Model Template

Information Regulator / IR

- POPIA provides for the establishment of an Information Regulator to regulate privacy and access to information.
- The IR is an independent body accountable to Parliament.
- The IR will also perform functions in terms of the Promotion of Access to Information Act 2 of 2000 as well as take over SAHRC functions.

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

Information Regulator: Powers and Duties

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

- Educate the public on POPIA;
- Monitor and enforce compliance;
- Issue codes of conduct which are sector specific (e.g. Assaf Code of Conduct) to be followed by Responsible Parties when processing information;
- Receive and investigate complaints;
- Mediate in matters;
- Conduct research on policies and regulations nationally and internationally to advance the protection of Personal Information.

Enforcement

- An aggrieved data subject may lodge a complaint with the IR;
- The IR may investigate a complaint if they are of the opinion that a complaint should be investigated;
- The IR may refer a complaint to another body if the complaint, in whole or part, falls within the jurisdiction of another body.

Background of POPIA and the *working draft* CoC

Background of POPIA

- Commencement Date - 01 July 2020
- 1 year grace period or compliance
- Implementation Date - 01 July 2021

Assaf Steps to create a Code of Conduct fit for purpose -

- POPIA Chapter 7 makes provision for the development of Codes of Conduct to provide guidance on the interpretation of POPIA in relation to a particular sector or industry, or class of information
- Once approved by the IR and comes into force, it is legally binding
- CoC are to be revised and improved annually or upon request.
- Demonstrates how the research sector will ensure compliance with all conditions for lawful processing, this a working draft CoC

Progress of the *Working Draft* CoC

1. **2020 – 2 Open discussions - Open Science Week & Science Forum**
2. **February 2021 – Call for written inputs**
3. **03 May 2021 – POPIA Public Consultation Forum – 700 participants**
4. **13 May 2021 – Assaf POPIA Discussion Forum with the NHREC**
5. **18 May 2021 – Assaf & NHREC POPIA Stakeholder Engagement with RECs – 300 participants**
6. **20 August 2021 – Draft circulated to stakeholders for input September / October – Draft Code of Conduct text being finalised**
7. **The text of the working draft Code of Conduct is being delibarted by the ASSAf Steering and Drafting Committees**
8. **Further consultation will take place with stakeholders in 2022 before submission to the IR**
9. **IR publish in the GG for public comment**
10. **IR and ASSAf review comments and finalise**
11. **IR approve and publish again in the GG (within 13 weeks of receiving it)**
12. **2 Publications in SAJS**
    - i. **Drafting a Code of Conduct for Research under the Protection of Personal Information Act No. 4 of 2013**
    - ii. **POPIA Code of Conduct**

Currently: New Updated version is being finalized and will be shared with stakeholders in the coming weeks for consultation before it is submitted to the IR. Renewed emphasis on anonymising the information or including satisfactory safeguards in DTA to ensure that the information is secure and that further processing is controlled.

Assaf *Working Draft* Code of Conduct for Research and Why?

POPIA Chapter 7 makes provision for the development of Codes of Conduct to provide guidance on the interpretation of POPIA in relation to a particular sector or industry, or class of information

Codes of Conduct are living laws that can be revised and improved periodically or upon request.

Why a Code of Conduct is needed?

- Unclear how the principles will apply in practice to research
- POPIA provides certain exceptions from the lawful conditions of processing Personal Information for research, how and where do they apply
- Uniform approach to the regulation of Personal Information for research across all government departments, academic institutions, research councils and the private sector
- To alleviate the need for the research sector to apply for prior authorisations

Why ASSAf?

- Sufficiently representative of research and researchers in South Africa
- Complementary to USAf Document which is a broader Code of Conduct and not specific to research

Scope of the *Working Draft* Code of Conduct

- Applies to: industry and academia
- Academic or scholarly research of all disciplines that uses, collects, processes and stores, Personal Information as part of the research process.
- Research: broadly, the generation, preservation, augmentation, and improvement of knowledge by means of investigations and methods pertinent to the scientific or disciplinary, and which is mindful of the value of knowledge for the betterment of society, including open science.

Relation to Other Legislation and Regulatory Frameworks

- **Bill of Rights: 'Everyone has … the right not to be subjected to medical or scientific experiments without their informed consent'**
- **National Health Act and 2015 DoH Guidelines on Ethics in Research:**
  - Applies to research in a broad sense, not strictly health research
  - Consent of the individual involved for research projects that involve human participants
  - Health ethics committees to be registered with the NHREC
  - International standards: open science and data protection law in the African Union and European Union (GDPR)
- **POPIA compliance does not mean that ethics standards have been met, and meeting ethical standards for research does not mean that POPIA Compliance has been met.**

Lawful Basis

- All processing of Personal Information must have a lawful basis
- ***Only collect data that is relevant and answers research questions / research protocol / proposal***
- Cannot change lawful basis during processing
- Consent: limitations, can be withdrawn
- Performance of a duty in law: e.g. science councils established through Acts of Parliament, or the National Health Laboratory Services
- Necessary for the fulfilment of the legitimate interests of the responsible party. For a research institution, the legitimate interests would include research.

Consent

- Consent must be specific, free and informed
- Further processing allows for the re-use of Personal Information for a secondary purpose related to the original purpose of collection, where safeguards are in place to ensure the information is only used for research and is not published in an identifiable form.
- Collection from the Data Subject: except where the Personal Information is already contained in a public record, where it is for research purposes or where it is reasonably impractical.

Consent Requirements

- When obtaining consent from Data Subjects, express consent needs to be obtained for:
  - Collecting and processing the Personal Information by the Responsible Party for the stated purpose;
  - Storing the Personal Information with information provided on the safeguards and security measures in place to protect the Personal Information and the rights of the Data Subject;
  - Sharing the Personal Information with a third party or another Responsible Party, if relevant;
  - Transferring the Personal Information outside of South Africa, if relevant;
  - The future use of the Personal Information for research purposes; and
  - The de-identification of their Personal Information for use in further data processing activities.

Governance of the *Working Draft* Code of Conduct

- Research institutions, through their Information Officers, will need to report annually to ASSAf on compliance with the Code and complaints received in relation to the Code.
- ASSAf will handle complaints in relation to the Code, in terms of the complaints handling guidance provided by the IR.
- The Code will be a living law, subject to regular review by all stakeholders involved.

Complaints Handling Procedure

- Complainant first takes case to the Responsible Party (IO investigates and can refer to/consult with the REC that approved the study)
- If aggrieved, complainant takes complaint to ASSAf who appoints an independent adjudicator to review the case
- ASSAf can refer the case to another body better suited to investigate, e.g. NHREC
- If aggrieved, complainant takes case to the Information Regulator

Violations Penalties

- Serious POPIA violations
- Fine of up to R10 million; or
- 10 years in jail

Data Breaches Examples

- Veeam Data Protection Trends Report 2022 uncovered that 86% of South African organisations suffered ransomware attacks, making cyber-attacks one of the single-biggest causes for downtime for the second consecutive year
- *"Research has revealed the top 10 countries losing the most money to data breaches and South Africa features in 9th place with an average data breach cost of R58 million in 2021, research by tech firm Proxyrack showed."*

Data Breaches Examples

- Experian - a consumer, business and credit information services agency – has experienced a breach of data which has exposed some personal information of as many as 24 million South Africans and 793 749 business entities to a suspected fraudster
- Sept 2021 - A ransomware attack at the Department of Justice and Constitutional Development (DOJ&CD) potentially breached over 1,200 confidential files containing personal information
- Dis-Chem said an unauthorized party accessed personal details of 3,687,881 customers, including names, email addresses and cell phone numbers.

Compliance with POPIA and the *Working Draft* Code of Conduct

- Recording POPIA compliance in data management plans:
  - What is the lawful basis for processing?
  - Who is the responsible party?
  - Risk assessment and where high risk, a full personal information impact assessment
  - Consent process
  - Risk model for research ("what are the potential harms of my study and how can I mitigate them" - overlap between law and ethics)
  - What type of personal information is being processed, e.g. high risk?
  - Transfers outside of South Africa
  - Use of information matching programmes
  - Consent and safeguards
  - Level of de-identification of the Personal Information

The POPIA *Working Draft Code of Conduct* – Practical Implications for Researchers and RECs

REC Mandate

Perception of what RECs need to do:

- Mandate for ethical review, protecting participants, promoting justice, access, autonomy and empowerment
- Exact scope and nature of legal mandate often debated (Constitution, National Health Act, POPIA)
- Information giving and consent process, mandatory legal reporting requirements

  Practical Reality
- Researchers are turning to RECs for guidance on POPIA compliance.
- Researchers “expect” RECs to play some role

What happens without a Code of Conduct?

- Utilising existing regulatory infrastructure helps
- RECs are a common convergence point for a large amount of research, so it makes sense to propose RECs as A SAFEGUARD to POPIA, facilitating limitation of harms to participants
- But what are the implications for researchers, REC members and administrators?

Where does the ASSAf *Working Draft* Code of Conduct fit in, in Research?

- On an Institutional Level:
  - REC POPIA Compliance

    USAf POPIA Document – Abandoned Code of Conduct

- On a Researchers Level:
  - Research Project in terms of POPIA Compliance
    - Assaf POPIA *DRAFT* Code of Conduct

Supporting Guidance Documents

- RECs review is time consuming, often voluntary, and RECs and REC administrators are under pressure to turnaround applications speedily
- Creating a resource page on Assaf website to support compliance in practice with the Working Draft CoC
- Save time
- Uniformity and consistency
- Allow for a guidelines for RECs and researchers

- Potential kind of Supporting Guidance Documents

1. POPIA Information Sheet
2. POPIA Consent Form
3. Data Management Plan

POPIA Information Sheet

- Purpose:
  - When obtaining consent for the collection, use and storage of personal information from a data subject, the responsible party must ensure that they provide the data subject with all relevant information about their rights, why their personal information is being collected, and what will be done with it.
  - Goes over-and-above volume of info required in Study Information Sheet, but there is some overlap.
  - This is info the by law needs to be given to individuals participating in research studies when utilising their personal information for any purpose where you get their consent to participate.
  - Could either be a separate template that is given to research participants during the information and consent process OR could be a proposed wording that can be inserted into the overall Study Information Sheet.

POPIA Consent Form

- Speaks to the POPIA Information Sheet / POPIA Section of Study Information Sheet
- Required by law
- Could be separate form (similar to that sometimes used for future testing, genetic studies and sample storage) or could be part of the Study Consent Form (it would still require a signature from the participant) – international considerations.

Data Management Plan / Privacy Risk Assessment

Data Management Plan – storage, destruction, processing etc.

Rubric for various aspects of data management that researchers and RECs can consider

POPIA “Prompts” Compliance and thinking ahead

Level of inherent risk based on nature of information being processed

Data Management Plan / Privacy Risk Assessment

- Research Data Management Policy
- Purpose of Policy - Establish the minimum standards for the management of research data following international and local best practice. Accordingly, it will protect the interests of the University's academics and students with respect to research data. It will facilitate compliance with the needs of research funders. It will also provide the means to ensure that the maximum value can be obtained from valuable research data for the benefit of the broader communities serviced by the University.
- Ensure consistent research practice related to data management principles and practices that support effective data sharing. It will enable research data to be discoverable, accessible and reusable.
- Scope of Policy - Includes all research data generated at Wits. It provides a set of standards for the management of research data, which will improve the quality of our use and reuse of research data.

Data Management Plan / Privacy Risk Assessment

- Data Management Plan Template
- Different Stakeholders have different requirements e.g. funders, collaborators etc.
- Training
- Assistance with DMP
- Show example of DMP
- Research Data Lifecycle

Way Forward

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

POPIA The Protection of Personal Information Act: Unpacked

On 01 July 2020, the Protection of Personal Information Act, 2013 (POPIA) came into effect and governs the processing of personal information by public and private bodies across the board. The 12-month grace period for compliance commenced on 1 July 2020 effectively giving private and public bodies until 30 June 2021 to comply with the wide-ranging requirements of the Act.

What is the purpose of POPIA?

The purpose of POPIA is to balance a person's right to privacy which is enshrined in the Constitution against the right to access to information. The Act achieves this by regulating processing activities and by placing obligations on the persons/entities processing personal information.

Here's what you need to know:

Personal Information is broadly defined as information relating to an identifiable, living natural or juristic person ("Data Subjects"). As you can see POPIA refers to the personal information of juristic persons, which means that the University will be able to rely on POPIA to protect their data.

Processing of Personal Information by a responsible party/an operator includes actions such as requesting, collecting, storing and processing or otherwise using the Personal Information of a person/juristic entity and must be lawful and in compliance with the provisions of POPIA..

Definitions

A **Responsible Party (the University)** is the person or entity acting independently or jointly with other responsible parties that determines the purpose and means of processing Personal Information.

An **Operator (consultants/ entities appointed by the University)** processes personal information for, or on behalf of a Responsible Party in terms of a contract or mandate without being under direct control of the Responsible Party

Information Regulator is empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA.

The Responsible Party appoints Information Officer (the Registrar) whose responsibilities include

- Encouraging compliance by the University community with POPIA and ensuring lawful compliance with the conditions for the lawful processing of Personal Information;
- Attending to requests made to the University ito POPIA; and
- Assisting the Information Regulator with investigations conducted ito of POPIA.

The 8 Conditions for Lawful Processing

As prescribed by the Act

1 Accountability

The Responsible Party (the University) must ensure compliance with the provisions of POPIA. Operators must comply with the provisions of the contract concluded with a Responsible Party.

2 Processing Limitation

The Responsible Party (the University) must ensure that only relevant Personal Information is processed:

- lawfully; and
- in a reasonable manner that does not infringe the privacy of the individual

3 Purpose Specification

Personal Information must be collected (by authorised staff) for a specific purpose.

4 Further Processing Limitation

Further processing of Personal Information (i.e. for purposes other original purpose) must be in accordance and compatible with the original purpose of collection.

5 Information Quality

Practical and reasonable steps must be taken to ensure that the Personal Information is complete, accurate, not misleading and updated.

6 Openness

POPIA leans on the Promotion of Access to Information Act 2 of 2000 (PAIA). The purpose of PAIA is to allow access to any information held by the State, and any information held by private bodies that is required for the exercise and protection of any rights.

The Responsible Party must:

- **Maintain the documents of all processing operations under its responsibility ito PAIA.**
- **Take practical and reasonable to ensure that the Data Subjects are made aware:**
  - that their Personal Information is being collected;
  - where it is collected from;
  - how it will be used;
  - the details of the Responsible Party;
  - the purpose for which the Personal Information is being collected; and
  - consequences of non-compliance .

7 Security Safeguards

The Responsible Party must:

- Secure the integrity and confidentiality of Personal Information in its possession or under its control by implementing appropriate, reasonable, organizational, and technical measures to:
  - Identify all reasonably foreseeable risk;
  - Develop a compliance framework by taking cognizance of centralized, consistent and institute appropriate safety protocols/practices to mitigate against the identified risks.
  - Ensure that the safety protocols are reviewed and updated regularly.
- Ensure that its contracts with Operators contain provisions regulating the security measures by the Operator to preserve the integrity and confidentiality of the Personal Information.

8 Data Subject Participation:

Data Subjects have the right to access their Personal Information at no cost.

Provisions relating to Trans-Border Information

Restrictions apply to the transfer of personal information outside South Africa. Penalties apply to offences.

Security Compromises

Data breaches can be as a result of:

- human error (i.e. erroneously sending an email);
- theft of devices;
- system glitches;
- malicious/criminal activity which include inter alia
  - phishing attacks; or
  - cyber attacks.

Preparedness and Response Plan:

- develop a clear and effective incident/reporting plan in collaboration with the Dean of the Faculty or the Head of the Division, ICT, Finance, Legal and Human Resources and other relevant stakeholders;
- test internal responses to perceived/real breaches and implement a response protocol to minimize the risk. It would be prudent to engage with independent cyber security experts to restore the integrity of the information system or to upgrade the security protocols;
- create training/awareness programmes within the organization to encourage compliance with POPIA and to create a culture of compliance;
- develop a clear and concise notification plan to notify the Information Regulator as well as the Data Subjects. The notification must be made as soon as it is reasonably possible to do so after the discovery of the breach taking into account the legitimate needs of law enforcement or other measures to determine the nature and extent of the breach. The notification must be in writing or as directed by the Information Regulator.
- Operators must notify the Responsible Party immediately of any suspected or actual data breach.

Non-compliance

Non-compliance can result in serious consequences. The infringement of the provisions has far-reaching consequences such as a **hefty fine, 10 years imprisonment or both a fine and imprisonment.**

Protection of Personal Information: Remote workplace tips

The COVID-19 pandemic has forced employers to rethink and to stretch their workplace policies and to become more flexible by directing staff to work remotely increasing the risk of security breaches and data leaks which can compromise identities and personal information thus adding another dimension to the organization's responsibility towards ensuring compliance with POPIA. Employees now bear the responsibility to also ensure that the Personal Information is protected.

Useful Tips:

- All information taken/accessed offsite must be handled safely and securely.
- Only copies of documents which are absolutely essential for carrying out duties may be removed with the express written approval of the line manager. The originals must remain on-site.
- An accurate and updated register setting out the details of the employee, description of the document, reason and time of removal of must kept by the line manager.
- The documents must be stored in a safe/ secure cupboard/area.
- If there is travel involved then the documents must be placed in sealed bag and should remain under the supervision of the employee at all times.
- Laptops, computers and cellphones must be password controlled and the Personal Information must be encrypted.
- Only software approved by the ICT Department must be used and anti-virus software and personal firewalls must be installed and updated regularly.
- Computers or laptops should be logged off when unattended.
- All participants in a video conference must be notified of the purpose of the meeting and must consent to the meeting being recorded.
- Switch off cameras and microphones when not in use. Remove any personal/ business information from view when using the camera/during screen sharing.
- Work related email accounts must only be used for work related purposes.
- All files must be encrypted.
- It is the employees duty to ensure that emails are sent to the correct recipients.

Compiled by

Shobhna Morar

Batina Flemming

Tasneem Wadvalla

These are guidelines only. They are designed to assist you in ensuring compliance with POPIA. If you have any queries or difficulties please contact Mr Nkosinathi Mavimbela at the Legal Office: Nkosinathi.Mavimbela@wits.ac.za 0117171307.

UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG

100 1922 2022

Rapid Technology Developments

- What is your University Policy, stance?
- Chat GPT, Open AI, Microsoft etc. – POPIA Compliance

ChatGPT banned in Italy over privacy concerns

1 day ago

OpenAI launched ChatGPT last November

By Shiona McCallum
Technology reporter

Italy has become the first Western country to block advanced chatbot ChatGPT

Final Comments

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

- Application and Implementation of POPIA will be assisted by the Code of Conduct
- Code of Conduct de-codifies POPIA
- Be practical in applying POPIA and the working draft Code of Conduct
- Aiming for integration, and to streamline POPIA and research processes
- Collective commitment to the process and acknowledgement of the Code of Conducts fluidity
- The Code of Conduct once approved will assist in the compliance, application and implementation of POPIA

- **Acknowledgment – REASA Webinar presentation
- ** Acknowledgment – Wits University Registrar – Mrs. Carol Crosley
- **Acknowledgment – Assaf Drafting Team

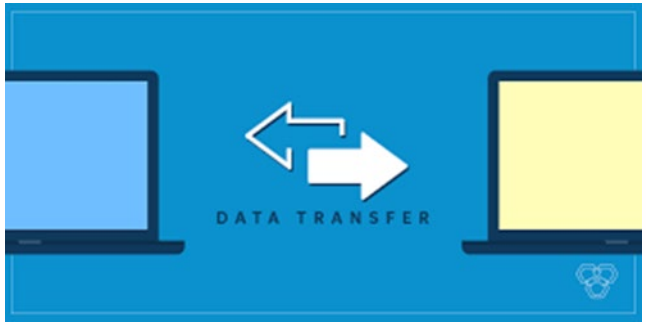

FAIRNESS
STEWARDSHIP
RESPECT
ACCOUNTABILITY
TRUST
SUPERVISION
DISCUSSION
HONESTY


Research
Integrity
environment
subjects
animals
Transparency
conclusions
presenting
communicating
practice
procedures
excellence
acknowledging
researchers
protocol
scholarship
methods
reporting
results
appropriate
performing
data
work
stewardship
generations
findings
including
making
gathering
interpretations
communication
drawing
participants
interpretation

THANK YOU


TRUSTED
RESEARCH


KEEP
CALM
AND TRUST ME
I'M A RESEARCH
SCIENTIST


DATA TRANSFER