POPIA@UCT
MORE ANSWERS THAN QUESTIONS

WE HOPE!

17 MARCH 2022

Project: **UCT POPIA COMPLIANCE PROJECT**
Client: **UCT**
Prepared by: **ELIZABETH DE STADLER**

novation consulting

POPIA IS NOT NEW.

(ANYMORE.)

WHAT HAS HAPPENED

- **POPIA came into force:** Last year, so it is not really ‘new’ anymore.
- **Scrutiny and audit findings:** Organisations are under pressure (from the IR, but also each other).
- **UCT responded:** A POPIA project was launched and a Data Privacy Policy was approved.
- **A research code of conduct is coming:** ASSAf is going to accredit a Code of Conduct for Research.

THE USAF GUIDELINE

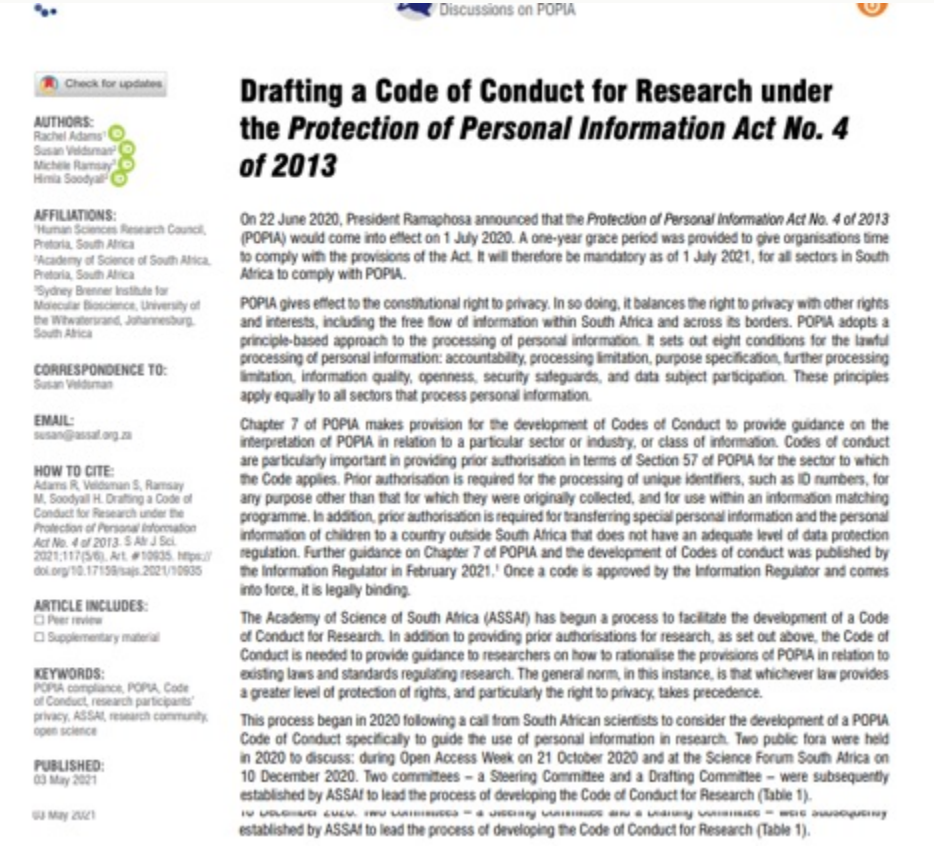
UNIVERSITIES SOUTH AFRICA

POPIA INDUSTRY CODE OF CONDUCT: PUBLIC UNIVERSITIES

A guide to implementing the POPIA

UNIVERSITIES SOUTH AFRICA

A RESEARCH CODE IS COMING…



Check for updates

AUTHORS:
Rachel Adams[1]
Susan Veldsman[2]
Michèle Ramsay[3]
Himla Soodyall[2]

AFFILIATIONS:
[1]Human Sciences Research Council, Pretoria, South Africa
[2]Academy of Science of South Africa, Pretoria, South Africa
[3]Sydney Brenner Institute for Molecular Bioscience, University of the Witwatersrand, Johannesburg, South Africa

CORRESPONDENCE TO:
Susan Veldsman

EMAIL:
susan@assaf.org.za

HOW TO CITE:
Adams R, Veldsman S, Ramsay M, Soodyall H. Drafting a Code of Conduct for Research under the *Protection of Personal Information Act No. 4 of 2013*. S Afr J Sci. 2021;117(5/6), Art. #10935. https://doi.org/10.17159/sajs.2021/10935

ARTICLE INCLUDES:
☐ Peer review
☐ Supplementary material

KEYWORDS:
POPIA compliance, POPIA, Code of Conduct, research participants' privacy, ASSAf, research community, open science

PUBLISHED:
03 May 2021

03 May 2021

Drafting a Code of Conduct for Research under the *Protection of Personal Information Act No. 4 of 2013*

On 22 June 2020, President Ramaphosa announced that the *Protection of Personal Information Act No. 4 of 2013* (POPIA) would come into effect on 1 July 2020. A one-year grace period was provided to give organisations time to comply with the provisions of the Act. It will therefore be mandatory as of 1 July 2021, for all sectors in South Africa to comply with POPIA.

POPIA gives effect to the constitutional right to privacy. In so doing, it balances the right to privacy with other rights and interests, including the free flow of information within South Africa and across its borders. POPIA adopts a principle-based approach to the processing of personal information. It sets out eight conditions for the lawful processing of personal information: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. These principles apply equally to all sectors that process personal information.

Chapter 7 of POPIA 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 particularly important in providing prior authorisation in terms of Section 57 of POPIA for the sector to which the Code applies. Prior authorisation is required for the processing of unique identifiers, such as ID numbers, for any purpose other than that for which they were originally collected, and for use within an information matching programme. In addition, prior authorisation is required for transferring special personal information and the personal information of children to a country outside South Africa that does not have an adequate level of data protection regulation. Further guidance on Chapter 7 of POPIA and the development of Codes of conduct was published by the Information Regulator in February 2021.[1] Once a code is approved by the Information Regulator and comes into force, it is legally binding.

The Academy of Science of South Africa (ASSAf) has begun a process to facilitate the development of a Code of Conduct for Research. In addition to providing prior authorisations for research, as set out above, the Code of Conduct is needed to provide guidance to researchers on how to rationalise the provisions of POPIA in relation to existing laws and standards regulating research. The general norm, in this instance, is that whichever law provides a greater level of protection of rights, and particularly the right to privacy, takes precedence.

This process began in 2020 following a call from South African scientists to consider the development of a POPIA Code of Conduct specifically to guide the use of personal information in research. Two public fora were held in 2020 to discuss: during Open Access Week on 21 October 2020 and at the Science Forum South Africa on 10 December 2020. Two committees – a Steering Committee and a Drafting Committee – were subsequently established by ASSAf to lead the process of developing the Code of Conduct for Research (Table 1).

10 December 2020. Two committees – a Steering Committee and a Drafting Committee – were subsequently established by ASSAf to lead the process of developing the Code of Conduct for Research (Table 1).

POPIA BASICS

(WHAT IS POPIA ABOUT?)

WHAT IS PERSONAL INFORMATION?

- Identifiers
- Demographic information
- Contact details
- Financial information
- Background or historical information

Information relating to an identifiable, living, natural person or an existing organisation.

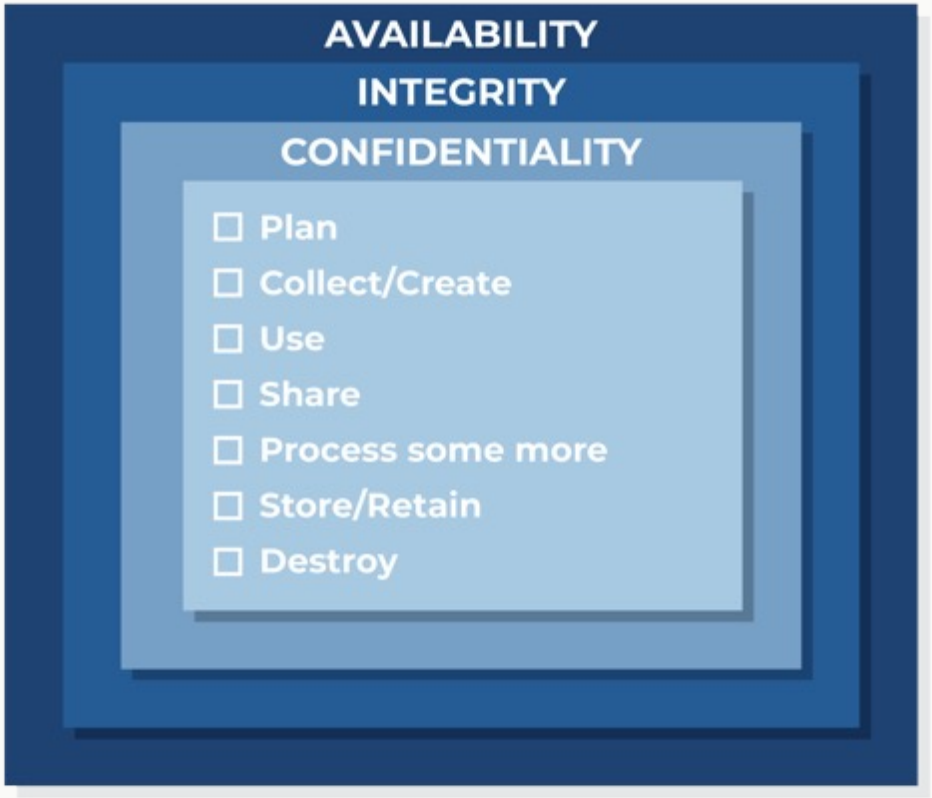
- Usernames and social media handles
- Biometric information
- Health information
- Preferences and opinions
- Behavioural information
- Correspondence

MEET YOUR DATA SUBJECTS

- **Students:** Prospective students, student applicants, students (South African or international), exchange students and alumni
- **Employees and functionaries:** Academic and administrative staff, employment candidates, external members of committees, student employees (e.g., research assistants, tutors), the SRC and council members
- **Research:** Researchers and research participants
- **Affiliated organisations:** Donors, funders, 'subsidiaries' (e.g., units and centers, companies in which the University is a shareholder), partners (e.g., exchange programmes), service providers, suppliers, independent contractors
- **Other individuals:** Family members of students and employees, sureties, emergency contacts visitors and members of the public

WHAT IS PROCESSING?

Processing activities lie at the heart of POPIA. A processing activity is a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored or destroyed. **Can you think of any?**



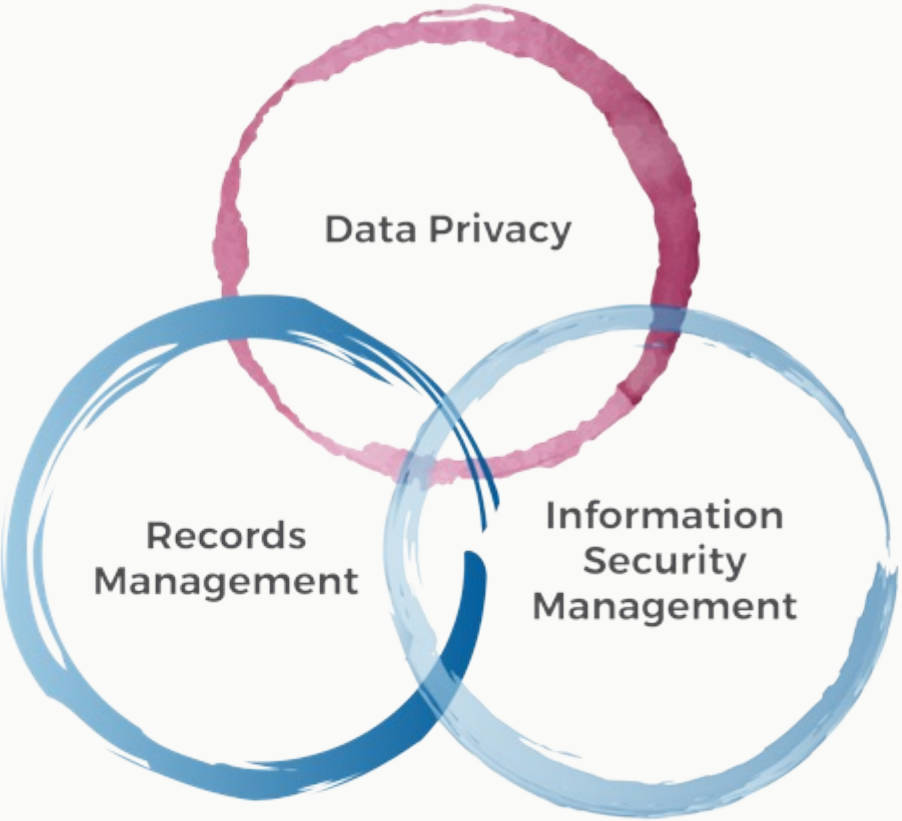
AVAILABILITY

INTEGRITY

CONFIDENTIALITY

- □ Plan
- □ Collect/Create
- □ Use
- □ Share
- □ Process some more
- □ Store/Retain
- □ Destroy

POLICIES ARE REQUIRED



- **Data Privacy Policy:** An interim one has been approved
- **Information Security Policy:** Approved by Council in May 2020. The POPIA Programme will aid in its implementation.
- **Records Management Policy:** Under review, but don’t start tossing things.
- **Research Policies:** Will be reviewed against draft ASSAf Code and POPIA.

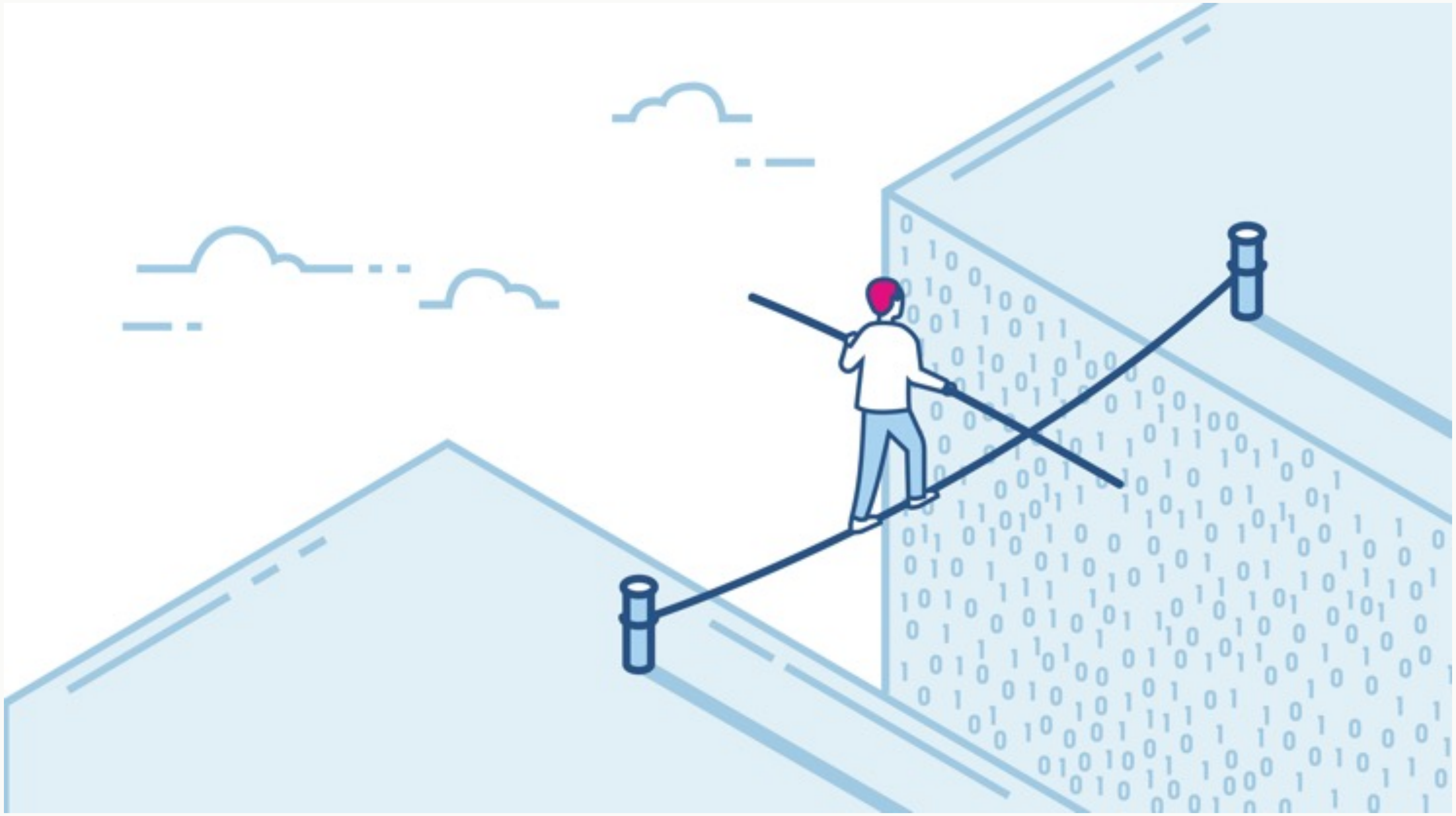
LET'S BREAK IT DOWN

(SOME RULES OF THUMB. AND BUSTING SOME MYTHS.)

POPIA IS ABOUT BALANCE

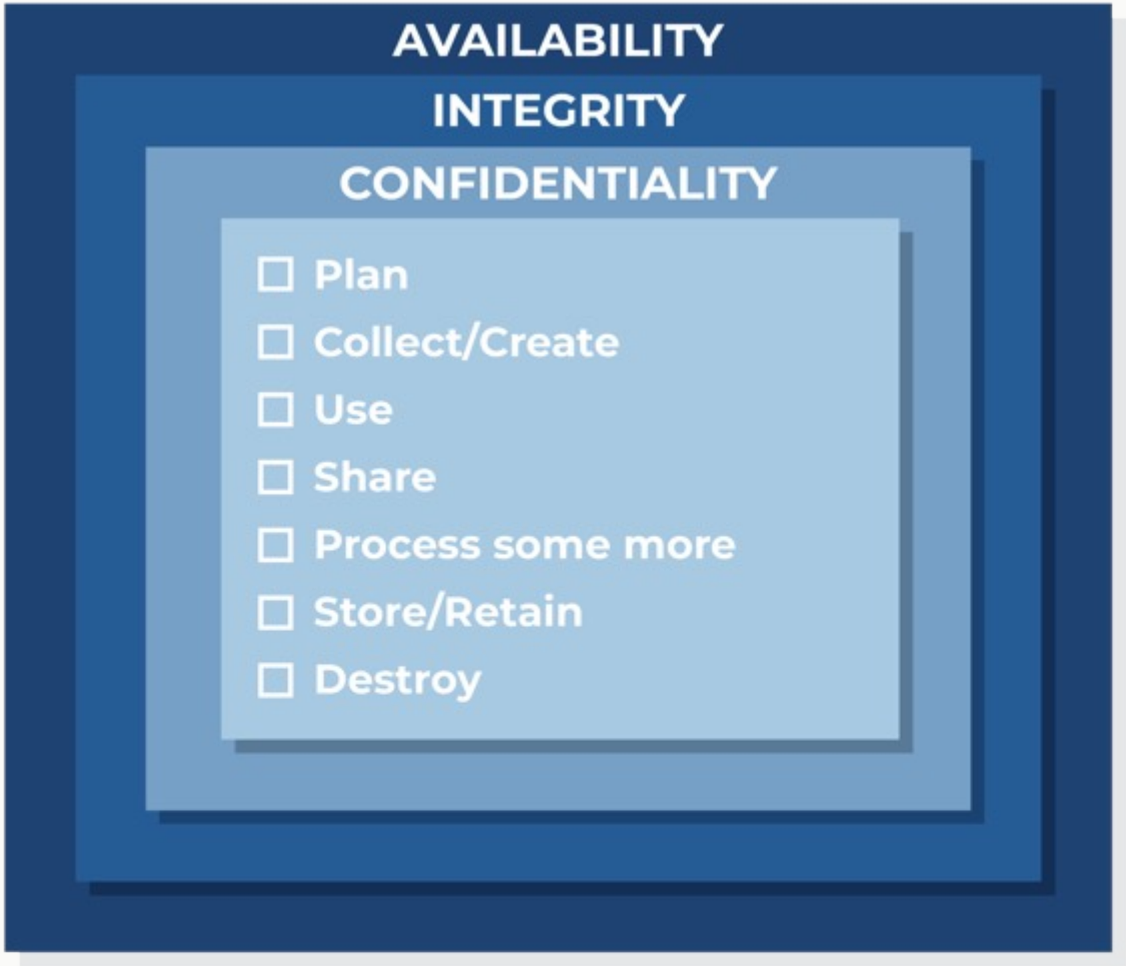
PRIVACY	BUSINESS
Protect the constitutional right to privacy including the unlawful collection, retention, dissemination and use of personal information (the preamble)	But, the Regulator must take into account the interests of public and private bodies in achieving their objectives (yes, even the commercial ones) in an efficient way (section 44(1)*(b)*)

POPIA IS ABOUT BALANCE



RULES OF THUMB

- Less is more
- No surprises
- Don’t share without protection
- Check yourself before you wreck yourself
- Use it or lose it
- Destroy it, don’t spread it
- Above all, keep it safe!



AVAILABILITY

INTEGRITY

CONFIDENTIALITY

□ Plan
□ Collect/Create
□ Use
□ Share
□ Process some more
□ Store/Retain
□ Destroy

ALSO DO A POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Know who is accountable: Are you sure that you know who is the responsible party and who is the operator?	• There is sharing, but no contract • There is a contract, but it does not state who is the responsible party
Document compliance: Is the processing activity written down?	• You cannot find out how it works • The process has not been documented • Or, it has been documented, but not recently
Purpose specification and provide a legal basis: Is this legal? Has someone checked that you have a legal basis?	• Purposes have not been specified in writing • Legal basis has not been documented

POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Keep processing to a minimum: 'Less is more' is a key principle of POPIA. Are you over-collecting or over-processing?	• You haven't done a form analysis • You didn't ask 'what do we use this for?' for each field • You collect the same information over and over • You haven't asked 'HMW do this more efficiently?'
Obtain information from legal sources: Where did we get the personal information from? Is it legal?	• You don't know where the information comes from. • You have not assessed whether the alternative source is legal.

POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Transparency: ‘No surprises’ is a key principle of POPIA? Do data subjects know what you are doing with their information?	• No privacy notice, no processing! • You haven’t checked that there is a privacy notice and that it covers the process in question • There is a privacy notice, but data subjects don’t know about it

POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Ensure information quality: Ask, ‘how do we make sure that information is (and stays!) complete, accurate, up to date and not misleading	• You collect information over and over again • Your systems don’t speak to each other • You don’t practice master data management (or know what it means) • You don’t assess the quality of the information

POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Limit sharing: Name the 'third parties' (people other than us or the data subject) with whom information is shared? Do you have contracts in place with these third parties	• You don't know who it is shared with (there is no record) • You haven't determined whether it is legal to share the information (go back to this slide) • You know there is sharing, but there is no record of a contract or you don't know whether there is a contract • There is a contract, but it doesn't say anything about how the personal information should be handled and what it can be used for

POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Keep it secure: Is the information protected against breaches of confidentiality, failures of integrity and interruptions of availability?	• You are not thinking about it at all • You think that security is ITs responsibility (so the process has not been assessed) • You don’t realise personal information is confidential • The personal information is all over the place (and you don’t know who has access) • You are not on top of your cyber-hygiene (e.g., updates, passwords, phishing, unapproved technology)

POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Records management: When does the relationship with the data subject end? For how long do you need to keep the information in use? Once it is not 'in use' what records do you need to keep?	• You keep everything forever • You can never find anything • When you find it, you don't know what version it is • Your records retention schedule is a list of legislation with retention periods

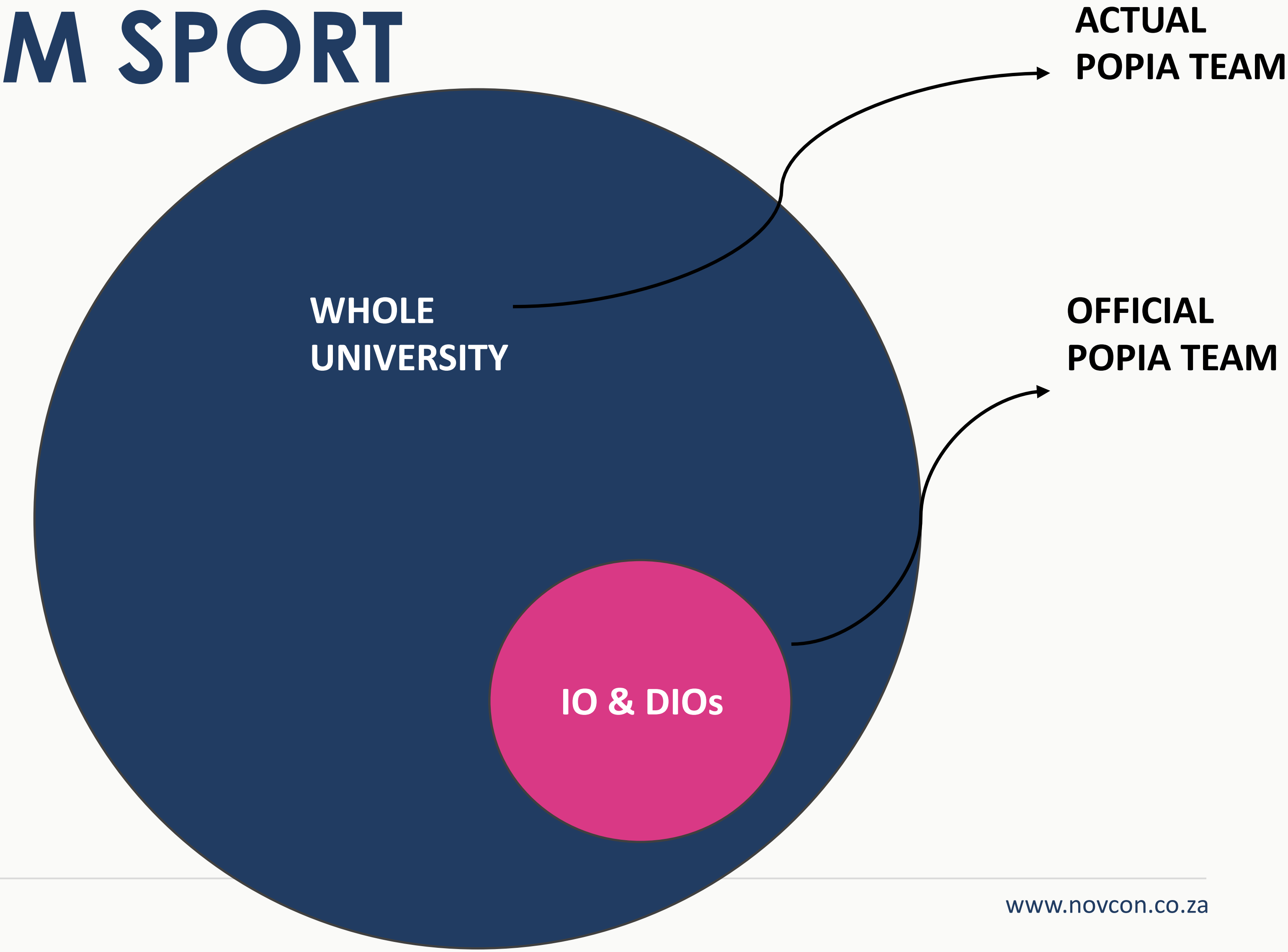
POPIA RISK IDENTIFICATION

THE QUESTION	SIGNS OF TROUBLE (YOU ARE NOT ON TOP OF THIS)
Data subject participation: Can you process the following requests accurately and (reasonably) quickly: • What information do you have about me? And who had access to it? • Delete my information! • Please correct my information • I want to object to how you are processing my information. • I want to withdraw the consent I gave for you to… • I want to make representations about an automated decision	• You don't know what information you keep where, what you use it for and who you shared it with • There is no process to update information in all of the places it is stored (master data management again!) • You don't have a process to handle data subject requests • Consents are not management in a central place • You don't know when you are allowed to delete things

POPIA IS A TEAM SPORT

(ROLES AND RESPONSIBILITIES.)

POPIA IS A TEAM SPORT



ROLES AND RESPONSIBILITIES

- **Information Officer:** The Vice-Chancellor.
  - It doesn't look like this can change.
  - The Information Officer *ensures* that POPIA responsibilities are discharged
  - Accountable (sometimes directly) to the Information Regulator
  - Must be registered registered with the IR
- **Deputy Information Officer(s):** Registrar, DVC: Research, COO
  - *Performs* the responsibilities of the Information Officer
  - It is a formal appointment which must be registered with the IR
  - Supported by a team of POPIA/PAIA compliance officers

ROLES AND RESPONSIBILITIES

- **Deans & directors:** The first line of defence & responsible for implementing policies in their areas.
- **Employees and students:**
    - Spread the word.
    - Ask for advice if you are uncertain about the personal information you are handling.
    - Report incidents immediately.
    - Participate in training when asked.

ANY HIGH RISK AREAS?

What are you most worried about?

BUT WAIT THERE'S MORE

(IT IS JUST TRAINING.)

NEXT TIME

- POPIA for Researchers
- New rights in terms of POPIA
- When can you share personal information?
- When the POPIA hits the fan: Who is going to jail?
- Securing personal information: The basics

THANK YOU!

popia@uct.ac.za