

Draft Frequently Asked Questions – POPIA Framework for Researchers and Research Institutions

Background

The POPIA Compliance Framework for Research is a set of voluntary, practical guidelines developed to help researchers, research institutions, and ethics committees interpret and apply the Protection of Personal Information Act (POPIA) in the context of research activities. It is not a legally binding document but offers widely endorsed guidance aligned with POPIA requirements.

The Framework was initiated and led by the Academy of Science of South Africa (ASSAf), drawing on its mandate to provide evidence-informed guidance on matters of national importance. ASSAf took the lead in response to the sector-wide need for a shared understanding of how POPIA applies to research. The initiative was supported by the Department of Science and Innovation (DSI) and involved extensive consultation with universities, science councils, legal experts, ethics professionals, and civil society representatives.

Importantly, the Framework reflects a broad consensus across South Africa's research community, including major research institutions, expressing the need for a coordinated and context-sensitive guidance to promote POPIA compliance while safeguarding the constitutional right to academic freedom and the public value of research. Although the initial proposal to accredit a formal Code of Conduct under POPIA was not pursued due to concerns about enforceability and inclusivity, the Framework serves as a flexible, evolving tool to support responsible research practice.

General Framework

1. What is the POPIA Compliance Framework for Research?

It is a voluntary, non-legally binding guideline developed to help researchers and institutions comply with the Protection of Personal Information Act (POPIA) in the context of research activities. It ensures personal information is processed lawfully, ethically, and transparently in research.

2. What is the purpose of adopting a non-legally binding Framework?

It provides clear and practical guidance to assist researchers in understanding how to implement POPIA requirements, which are legally binding. It further provides information on implementing safeguards for personal information and promotes ethical and lawful research practices. While the Framework is not legally binding, it is strongly recommended, as adopting its principles will reduce legal and reputational risks and ensure consistency across the research sector.

This Framework does not replace existing institutional policies or processes for POPIA compliance. Rather, it serves as a complementary guide to support alignment across institutions, while respecting their internal governance structures and obligations.

3. Who should use the Framework?

Researchers, research institutions and/or operators processing personal information on behalf of researchers.

4. How does the Framework support researchers and institutions?

It aligns POPIA requirements with research ethics and practices, providing clear principles, sample clauses, and workflows to safeguard data subject personal information without unnecessary burden.

5. Does the Framework create new barriers for research?

No, it supports rather than restricts research. It integrates legal and ethical standards already expected of researchers, and non-compliance with such standards could expose institutions to complaints or sanctions.

Consent and Participation

6. What is research consent and how is it different from POPIA consent or ethics clearance?

- **Research informed consent** - Participant voluntarily agrees to participate in research after being informed about its nature, risks, benefits, and data use.
- **POPIA consent** - Specific agreement to the processing of personal information, in line with POPIA.
- **Note:** Both research informed consent and POPIA consent may be required for a research project. They serve different legal and ethical purposes and could be combined in a single consent document (with multiple tick boxes or questions) or in two separate documents.
- **Research Ethics clearance** - Approval by the Research Ethics Committee (REC) that the study meets ethical standards.

7. Is blanket or opt-out consent allowed?

No, POPIA requires active, specific, informed consent (opt-in). Blanket consent or opt-out models are generally unacceptable, except under exceptional, REC-approved circumstances.

8. Is broad consent allowed?

Yes. Broad consent for the future use of personal information is permitted. It is good practice to state this in the information sheet and to ensure that adequate safeguards are in place. (For example that a new use of the data will need to be assessed and approved by a REC).

9. What if consent cannot be obtained (e.g. deceased participants / historical data etc.)?

POPIA allows for processing without consent if it's for a legitimate research purpose and no feasible way exists to obtain consent. This must be justified in the ethics application, with appropriate safeguards in place.

10. Can participants withdraw their data after consent?

Yes, unless the data has been irreversibly anonymised or already included in published findings. Participants must be informed of this upfront in the information sheet.

11. Is there a minimum age for giving consent under POPIA?

Yes. POPIA requires parent / guardian consent for processing information of children under 18 years of age, unless a legal exception applies or the Information Regulator has authorised the processing.

12. Do RECs need to assess participant understanding?

No, this is not required. However, it is recommended that participant understanding is assessed (e.g. through educational level and age appropriate language assessment) in high-risk or complex studies (e.g., involving emerging technologies such as artificial intelligence) to ensure truly informed consent.

13. What about participants who want to be identified in research (e.g., ethnographic)?

POPIA allows it if explicit, documented consent is given. Researchers must still protect other aspects of data use.

Data Processing and Sharing

14. What does pseudonymisation of data mean and how is it different to de-identification?

Pseudonymisation means that personal information is processed in such a way that the personal information can no longer be attributed to a specific research participant without the use of additional information, provided that such additional information is kept separately, confidential and secure from unauthorised access.

For example:

- Pseudonymised data: "John Smith" is replaced with "Participant 001", and the list linking John Smith to Participant 001 is stored separately and securely.
- De-identified data: All direct and indirect identifiers are removed or altered so that there is no reasonable way to re-identify the individual. In this case, the link to John Smith is permanently broken.

When the direct identifiers have been eliminated or transformed, but indirect identifiers remain intact, personal information has been pseudonymised and POPIA still applies. The information will be de-identified only once all direct and indirect identifiers have been removed or manipulated to break the link to real-world identifiers and POPIA does not apply.

If pseudonymised (re-identifiable) data are shared, access must be controlled through mechanisms like a Data Access Committee (DAC).

15. Can one use public social media content for research without consent?

Only if individuals have no reasonable expectation of privacy (e.g. public Twitter accounts), but even then, ethical considerations apply. Anonymisation and REC review are strongly advised.

16. Can biometric data (e.g., genetic data, fingerprints, facial images) be shared in open-access databases?

Biometric data requires special consideration as it's often inherently identifying as it is unique to an individual. However, it would still require linked personal data to identify the individual. Genetic data can rarely be truly anonymized due to familial links and advanced re-identification techniques. Such data should generally only be shared through controlled access mechanisms (like Data Access Committees) with strict governance, even if processed to remove direct identifiers. Open-access sharing of biometric data is generally not recommended unless exceptional circumstances justify it and robust legal safeguards exist.

17. Can non-biometric personal information be shared in open-access databases?

Yes, but only if properly anonymised/de-identified. Participants must give explicit consent for open-access use.

18. Is genetic/genomic data considered personal information?

Genetic information is derived from an individual's genetic material that can reveal health-related information, which is classified as special personal information.

Yes, it is personal information but only if it can reasonably be linked to an identifiable individual, even if the link is indirect or through advanced methods. Genetic/genomic data is only considered identifiable if it is linked through specific technical processing to other personal information that can directly or indirectly identify a living individual.

19. What safeguards should be implemented when processing special personal information?

The data should be pseudonymised or de-identified, access limited to only those who require it, and a risk assessment and legal justification documented, for example in research documents and ethics applications.

20. Does POPIA apply to biological samples?

Not directly. POPIA applies to recorded information about individuals, including data generated from samples, but not the physical samples themselves, unless linked to personal data or data records.

In South Africa, Material Transfer Agreements (MTAs) are used to govern the transfer/sharing of human biological material between contracting parties. To ensure sufficient data protection, MTAs should include contractual clauses that address the use and access of data related to such material being transferred/shared, consistent with POPIA.

21. Can data collected for one project be reused for new research?

Yes, data can be reused for new research, but only under specific conditions that ensure compliance with POPIA and ethical research standards.

When is reuse allowed?

- The new purpose must be compatible with the original consent.
- The data must not be published in an identifiable form.
- Reuse must comply with POPIA's purpose limitation and further processing requirements.
- Research participants must be notified where appropriate and practicable.

What conditions must be met?

A *legitimate interest assessment* (see Section 3.3.4) should be undertaken. Reuse is permitted when:

- The personal information will only be used for research purposes; and
 - The data will not be published in an identifiable form; or
 - The research serves a public interest and processing is necessary for that purpose;
- or

- It would be impossible or require disproportionate effort to re-contact participants for consent; and
- You can demonstrate that appropriate safeguards are in place and that reuse will not adversely affect the privacy of participants in a disproportionate way.

22. Can personal data be used commercially?

Commercial use of research data requires explicit consent obtained at the time of initial data collection. If participants did not originally consent to commercial use, new consent must generally be obtained before any commercial application. In exceptional circumstances where re-consent is impossible, researchers must demonstrate a legitimate interest under POPIA's conditions and seek both ethics committee and institutional legal review.

Special Considerations

23. How does the Framework support international collaboration?

By promoting standardised practices that are likely to align with those of foreign partners. Researchers must also comply with each jurisdiction's laws, but the Framework offers a strong foundation.

24. Is automated (made without human intervention) decision making allowed?

Yes, but with strict conditions. If the research involves automated decision-making that significantly affects participants (for example health or financial matters), participants must be clearly informed about the process, the logic in plain language, and be provided with an opportunity to challenge or respond to the decision.

25. How should consent be managed for vulnerable populations or indigenous communities?

Gatekeeper consent (e.g., from a chief or headman) may apply, but individual consent is still preferred. Often both are required. For stored samples without contactable participants, case-by-case assessment is needed. This is usually managed by the REC.

26. What guidance applies to cross-border data transfers within Africa (e.g., the SADC region)?

Data transfers within the Southern African Development Community (SADC) region are permitted under POPIA if the receiving country has adequate data protection laws or if safeguards (e.g., a Data Transfer Agreement) are in place. Researchers should check with their institution's legal or compliance office to ensure compliance with both POPIA and the receiving country's data laws.

Compliance and Governance

27. Should institutions revise their Research Data Management (RDM) policies?

Yes. Policies should align with POPIA principles and the Framework's guidance, covering collection, storage, sharing, and destruction of data.

28. How are complaints or breaches handled?

First reported to the institution or institutional REC. If unresolved, escalate to NHREC, and finally to the Information Regulator if necessary.

29. What security measures are expected?

Data should be classified by sensitivity and secured appropriately. POPIA encourages de-identification, anonymisation, or pseudonymisation where possible.

30. How long can data be kept?

As long as needed for the original purpose or as legally/ethically justified. Secure destruction should follow.

31. Can data be transferred abroad?

Yes, to countries with adequate protection laws or via contractual safeguards such as data transfer agreements. Researchers should check current guidance from the Information Regulator.

32. What is the role of the institution's Information Officer (IO)?

The IO holds ultimate legal responsibility for ensuring that the institution complies with POPIA. While the IO may delegate certain duties to Deputy Information Officers (DIOs), this does not absolve the IO of overall accountability. The extent to which IOs or DIOs are involved in reviewing research protocols may vary across institutions and is not necessarily a legal or ethical requirement. Researchers should refer to their institution's Promotion of Access to Information Act (PAIA) manual or equivalent documentation for details on the roles and responsibilities of the IO and any support structures in place.

33. Do retrospective studies or secondary data analyses require POPIA compliance?

Yes, even if data was previously collected, POPIA applies to any further processing. Researchers must ensure lawful grounds for use, such as consent or a legitimate research purpose, and ethics approval where applicable.

34. What happens if personal information is accidentally disclosed or mishandled due to negligence?

Any unauthorised access, disclosure, or loss of personal information, whether accidental or due to negligence, constitutes a potential data breach, misconduct, or unlawful processing. Such incidents must be reported immediately to the institution's Information Officer and the affected data subjects must also be notified, and the breach may need to be reported to the Information Regulator, in accordance with POPIA.

Institutions should have a clear breach response protocol to ensure timely investigation, mitigation of harm, and compliance with legal obligations.

35. What constitutes 'adequate' data security measures for research?

Adequate security measures depend on the sensitivity of the data. At a minimum, they should include password protection, encryption of digital files, secure physical storage for paper records, role-based access, and audit trails for data access. High-risk data (e.g., biometric/genomic) may require additional measures such as secure servers or controlled access via a Data Access Committee.

36. How should researchers handle data breaches during fieldwork?

Researchers must report any potential breach immediately to their institution's Information Officer (IO) or designated representative. Even in field settings, basic precautions (e.g., password-protected devices, locking field notes) should be taken. Incident

documentation, notification to affected individuals (if needed), and prompt containment are essential.

37. What are the penalties for POPIA non-compliance in research?

If convicted of an offence under POPIA (Section 107), a person may be liable to a fine not exceeding R10 million, imprisonment for a period of up to 10 years (depending on the severity of the offence), or both. Over and above criminal penalties, civil claims can be brought by affected data subjects for damages, and institutions may face significant reputational harm and internal disciplinary sanctions. Institutional sanctions may also apply.

38. How does POPIA apply to survey research and questionnaires?

Surveys that collect personal information must comply with POPIA. This includes ensuring informed consent, clarity on data use, and appropriate data storage. If the survey is anonymous and no identifiers are collected, POPIA may not apply, but ethical principles still do.

39. What documentation should researchers maintain to demonstrate POPIA compliance?

Researchers should keep copies of ethics approvals, informed consent forms, data management plans, de-identification logs, and any data-sharing agreements. This documentation serves as evidence of compliance during audits or investigations.

40. What is the relationship between institutional ethics approval and POPIA compliance?

Ethics approval evaluates the ethical integrity of research, including protection of personal information. However, ethics approval alone does not equal POPIA compliance. Researchers are responsible for ensuring that data processing meets POPIA's legal requirements, in addition to ethics standards.

Links to important documents

[ASSAf POPIA Compliance Framework for Researchers and Research Institutions](#)

[Protection of Personal Information Act \(POPI Act\)](#)

[Information Regulator](#)

[NHREC Guidelines](#) (South African Ethics in Health Research Guidelines: Principles, Processes and Structures, 2024, (V3.1) (NDoH 2024))

Acronyms

AI	Artificial Intelligence
ASSAf	Academy of Science of South Africa
DAC	Data Access Committee
DIO	Deputy Information Officers
DSI	Department of Science and Innovation

IO	Information Officer
NHREC	National Health Research Ethics Council
PAIA	Promotion of Access to Information Act
POPIA	Protection of Personal Information Act
RDM	Research Data Management
REC	Research Ethics Committee
SADC	Southern African Development Community

Glossary

For definitions of terms used in this FAQ, please refer to [Section 5: Glossary in the POPIA Compliance Framework](#).