



POPIA COMPLIANCE FRAMEWORK

For Researchers and Research Institutions

Table of contents

1. ABOUT THIS FRAMEWORK	3
1.1. The purpose of the framework	3
1.2. When the framework applies	3
2. WHO THIS FRAMEWORK APPLIES TO	6
2.1. Responsible parties	6
2.1.1. Responsible parties' responsibilities	7
2.2. Operators	7
2.2.1. Operator's responsibilities	8
2.3. Research institutions and independent researchers	8
2.4. The sections of the framework that apply to you	8
3. MAKING YOUR PROJECT POPIA COMPLIANT	9
3.1. Defining the purpose of your research	9
3.2. Privacy impact assessments	11
3.3. Having a legal justification	11
3.3.1. Asking the research participant for consent	12
3.3.2. The research is required by law	13
3.3.3. The research is conducted by a public body performing public law duty	13
3.3.4. The research is in your legitimate interest or that of a third party	14
3.3.5. When your research includes special personal information	15
3.3.6. When your research includes personal information of a child	16
3.4. Sourcing the personal information	18
3.4.1. The direct collection rule	19
3.4.2. Using previously collected data for new purposes	20
3.4.3. Minimal processing	22
3.5. Asking for POPIA consent	23
3.5.1. POPIA consent is different to research consent	23
3.6. Contacting participants	23
3.6.1. Asking for consent	23
3.6.2. Transparency and notification	24
3.6.3. Participants' rights	25
3.7. Collecting data	27
3.7.1. Adhere to your research document	27
3.7.2. Information quality	27

3.8. Storing data	28
3.8.1. Retention and restriction of records.....	29
3.9. Sharing personal information	30
3.9.1. How to assess whether you can share personal information.....	30
3.9.2. Sharing personal information with operators	30
3.9.3. Sharing personal information with other responsible parties	31
3.9.4. Transborder information flows	32
3.10. Publishing data for further processing	33
3.10.1. Using previously collected data for new purposes	34
4. POPIA COMPLIANCE FOR INSTITUTIONS AND INDEPENDENT RESEARCHERS	35
4.1. Your responsibilities	35
4.2. Monitoring and compliance with the framework	35
4.3. Accountability checklist	35
4.4. A three-phase research PIIA	37
4.4.1. Inherent risk assessment	37
4.4.2. Perform a self-assessment	39
4.4.3. Implementation and monitoring	40
4.5. Appropriate technical and organisational safeguards	40
4.6. Security compromises	42
4.7. Retaining records	44
5. Glossary	46

1. ABOUT THIS FRAMEWORK

1.1. The purpose of the framework

If you are a researcher (in an institution, commercial entity, or a private investigator), or [research](#) institution [processing](#) identifiable [personal information](#) in South Africa, you need to comply with the Protection of Personal Information Act ([POPIA](#)).

This framework guides **researchers** on what they should think about to ensure that their research projects comply with the Protection of Personal Information Act (POPIA). It aims to create **legal certainty** by helping researchers, but also committees (e.g. ethics committees), and institutions to have a consistent interpretation of POPIA and its impact on research.

The framework also sets out the steps **research institutions** must take to become POPIA compliant. It seeks to establish robust **safeguards** to protect research data (i.e. data that contains personal information) in South Africa. If you are an independent researcher not working under a research institution, those steps will also apply to you.

1.2. When the framework applies

If you answer 'yes' to **all** of the following questions, then this framework applies to you:

- Do you process **identifiable personal** information?
- Do you process identifiable personal information for **research**?
- Do you process identifiable personal information in **South Africa**?



What is processing?

Processing includes collecting, creating, using, sharing, transforming, storing, or preserving [research participants](#)' personal information.



What is personal information?

Personal information is any information related to an identifiable, living individual or an identifiable, existing juristic person (e.g., a company or other organisation). **Identifiable personal information** is information that can be used to identify a person, for example their name, ID number, online identifier, telephone number, or email address.



What is processing in South Africa?

This means that you are based in South Africa. If you are a foreign researcher, you are also considered to be processing in South Africa if you:

- use physical infrastructure, information technology infrastructure or human resources located in South Africa to process personal information;
- use equipment or technology in South Africa to process personal information; or
- collaborate with South African researchers to process personal information in South Africa.

If all the questions apply to your research, then this framework applies to you. You can continue to read the rest of the document.



NB: You should always consider all your legislative and ethical obligations, for example, if you are doing health research you must also comply with the National Health Act 61 of 2003. If this framework conflicts with a law, you must comply with the requirements that best protect the personal information of research participants.

- If not **all** of the questions apply to your research, this framework does not apply to you.
- If the personal information you work with has been **de-identified**, this framework does not apply.




What is de-identification?

De-identification means to delete personal information that identifies research participants, can be manipulated to identify them, or can be linked by a reasonably foreseeable method to other information that identifies them. De-identification is more difficult than it sounds, considering technological advancements and the fact that increasing volumes of personal information are in the public domain.

Biometric information, including genetic information, 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.

Even when no identifiers are collected, the research participant may still be identifiable through manipulation or linking.



You must:

- ✓ develop and implement standards to ensure effective de-identification;
- ✓ document to what extent the personal information has been de-identified; and
- ✓ document when a re-evaluation will occur to cater to changes in technology, the environment in which the de-identified information is stored, and what other information is available.

2. WHO THIS FRAMEWORK APPLIES TO

POPIA outlines different roles involved in processing personal information and outlines their respective responsibilities. According to Condition 1 of POPIA (accountability), it is important to clearly define who is responsible for what when processing personal information. Your accountability under POPIA will depend on your role.

This framework applies to responsible parties and joint responsible parties. These roles are described below.

2.1. Responsible parties



Section 1 - Definition of [responsible party](#)

Section 8 - Responsible party to ensure conditions for lawful processing

A **responsible party** is a private or [public body](#) or a person who, alone or with others, determines why and how to process personal information. The responsible party is liable for complying with POPIA from the moment the research begins until it is completed. A responsible party can act alone, or they can make joint decisions about why and how to process personal information with other responsible parties. When responsible parties work together in a processing activity, they may share joint responsibility and they are referred to as **joint responsible parties**.¹

If you are doing research, you will fall into one of these categories:

- You are a responsible party if you act independently in your research and not under the direction of an organisation.
- You are a joint responsible party if you and another person (such as a fellow researcher) or organisation (such as a university) make joint decisions about the purpose of the research and how it will be conducted. For example, if you need to submit a research proposal to a committee before you can start with your research, both you and the organisation to which the committee belongs are joint responsible parties. Since joint responsible parties are both responsible for processing personal information, the Information Regulator and research participants can choose which party to hold accountable to comply with POPIA. They may also decide to hold both joint responsible parties liable together. If you are a joint responsible party, you should enter into an agreement with the other

¹ See European Data Protection Board *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf); Global Alliance for Genomics & Health GA4GH GDPR Brief: *Are university-employed scientific researchers 'Data Controllers' for the purposes of the GDPR? (May 2020)* (<https://www.ga4gh.org/news/ga4gh-gdpr-brief-are-university-employed-scientific-researchers-data-controllers-for-the-purposes-of-the-gdpr-may-2020/>).

party or be subject to binding rules (e.g., in a policy or procedure) that clearly define who is responsible for compliance with specific parts of this framework.

2.1.1. Responsible parties' responsibilities

If you are not conducting the research alone, you must:

- ✓ conclude agreements and establish policies or other binding obligations with joint responsible parties that clearly defines who must comply with which sections of this framework;
- ✓ conclude agreements and establish policies or other binding obligations with all operators, in which the operator agrees:
 - to limit its use of personal information to instances where the responsible party gave written authorisation;
 - that the personal information must not be shared with [third parties](#) without the responsible party's written authorisation;
 - to comply with the security safeguards set out in section 4.5 in this framework;
 - to notify the responsible party immediately in the case of a security compromise;
 - to take any additional steps the responsible party requires to comply with this framework;
- ✓ comply with the guidelines on transborder information flows set out in section 3.9.4.



What does POPIA say?

POPIA does not clearly explain how responsibility for compliance will be shared. According to guidance under the EU Data Protection Directive, unless the parties or the factual situation suggest otherwise, both controllers will usually be held equally responsible.

2.2. Operators



Section 1 - Definition of [operator](#)

An **operator** is a private or public body or person who processes personal information on behalf of a responsible party, under a contract or mandate, but operates independently and is not under the direct authority of the responsible party. An example of an operator is a third-party service provider who you have enlisted to process personal information.

2.2.1. Operator's responsibilities

Operators have limited direct responsibilities regarding the processing of personal information. Operators:

- may only process personal information with the knowledge or authorisation of the responsible party;
- must treat the personal information which comes into their knowledge as confidential; and
- must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.



NB: There must be a written agreement between the responsible party and their operator. This agreement must state that the responsible party will ensure that the operator establishes and maintains appropriate technical and organisational security measures. See section 3.9.2.

2.3. Research institutions and independent researchers

Research institutions and independent researchers also have further responsibilities to ensure that they comply with POPIA. These responsibilities are set out in [section 4](#).

2.4. The sections of the framework that apply to you



If you are a **researcher** conducting research under a research institution or you are an independent researcher, [section 3](#) will guide you on making your research project POPIA compliant.



If you are a **research institution**, there are also steps that you need to take to make your organisation POPIA compliant. These steps are set out in [section 4](#). If you are an **independent researcher** not working under a research institution, the guidelines in [section 4](#) also apply to you.

3. MAKING YOUR PROJECT POPIA COMPLIANT

If you are a researcher conducting research under a research institution or you are an independent researcher, this section applies to you. This section takes you through every step of the research process and what you should think about to make sure that your research is POPIA compliant.



NB: If you are an independent researcher, you have additional responsibilities which are set out in [section 4](#).

3.1. Defining the purpose of your research



Section 13 - Collection for a specific purpose

One of the first steps in doing research is to define the purpose of the research. Most research institutions will ask you to draft [research documentation](#) that outlines your plan for your research study. These documents can be research proposals, data management plans, or similar documents. In your research documents, you must show the following information to comply with POPIA.

- **What personal information is being collected**
You must make a list of the personal information that you propose to collect.
- **The purpose, aim, or objective for collecting the personal information**
You must indicate why you are collecting the personal information; be specific and explicit. Anyone not involved in the research (such as the Information Regulator) should be able to clearly understand why you are collecting each piece of personal information.
- **The nature, extent, and context of the processing of personal information**
You must include the following in your research documents:
 - ✓ the number of research participants and how you will recruit and contact them;
 - ✓ how you will collect, use, and store personal information;
 - ✓ the type of personal information you will collect;
 - ✓ where you will collect the personal information from;
 - ✓ if you share the personal information, with whom you propose to share it (including external collaborators, other researchers in South Africa and internationally, industry partners, funders, service or system providers, and cloud hosting services) and the purpose for sharing it with them;
 - ✓ any concerns relating to the security of the personal information; and
 - ✓ whether any new or innovative technology will be used to process the personal information.



What does POPIA say?

Personal information includes any information that relates to an identifiable, living individual or any identifiable, existing juristic person (e.g., a company or other type of organisation).

POPIA provides the following examples:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.
- information relating to the education or the medical, financial, criminal or employment history of the person.
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or another particular assignment to the person.
- the personal opinions, views, or preferences of the person.
- 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.
- the views or opinions of another individual about the person.
- 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.

POPIA also defines special personal information, which requires an extra layer of requirements. Here are examples of special personal information:

- Religious and philosophical beliefs: For example, church membership, climate change denialism, or ethical veganism.
- Race or ethnic origin: For example, membership to a population group, culture, ancestry, territorial possession, language, or forms of dress.
- Trade union membership.
- Political persuasion: For example, membership to a political party, political opinions, or voting records.
- Health: For example, any information on physical or mental injury, disease, disability or disease risk, including medical history, medical opinions, diagnosis and clinical treatment; medical examination data, test results, data from medical devices, or data from fitness trackers; information collected from a research participant when they register for health services or access treatment; any appointment details, reminders and invoices which reveal the health status of a research participant; any other information or

behaviour that reveals a past, present or future physical or mental health status; administrative documents that reveal health status such as medical certificates, forms concerning sick leave or the reimbursement of medical expenses; inherited characteristics or genetic data.

- Sex life: For example, information about a research participant's sexual activity, relationships, sexual orientation, or sexual proclivities.
- Biometric information: The information that results from specific technical processing relating to the physical, physiological, or behavioural characteristics of a research participant, such as facial images or dactyloscopic or genetic data when it is linked with other personal information to identify a data subject.
- Criminal behaviour of a data subject relating to the alleged commission of an offence or proceedings relating to an alleged offence (Criminal convictions are not special personal information.)

The personal information of a **child** also has extra requirements under POPIA. POPIA defines a child as anyone under the age of 18 who is not legally competent to take any action or decision for themselves without the assistance of a competent person. Make sure to indicate if you use the personal information of a child.

3.2. Privacy impact assessments

Your research institution will have a Personal Information Impact Assessment (PIIA) in place that you need to complete to ensure that you manage the risk to research participants appropriately by including appropriate safeguards. Read more about the PIIA in section 4.4 and ask your research organisation if you do not know how to access the PIIA.

3.3. Having a legal justification

POPIA provides only six legal grounds for processing personal information, and at least one must apply for the processing to be lawful. There are stricter justifications if you are processing **special personal information** or the personal information of a **child**.



What does POPIA say?

Section 11 says that personal information can be processed if the:

- data subject consents;
- processing is necessary in terms of a contract;
- processing complies with an obligation imposed by law on the responsible party;
- 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 a third party to whom the personal information is given.



NB:

If you do not have a legal justification, then it is unlawful for the research to continue.

A research participant may also object to you processing their personal information, but only if you rely on certain legal justifications, See section 3.6.3.

3.3.1. Asking the research participant for consent

You should ask the research participant for [POPIA consent](#) to use their personal information where possible. However, it is just one of the legal justifications that you can rely on.

To comply with POPIA, the consent must include the following and be:

- ✓ **Voluntary:** Research participants should not be coerced into providing POPIA consent. You should take extreme care when offering incentives to ensure that you do not undermine the free will of the research participants, or exploit their vulnerability. Research participants must be able to withdraw their POPIA consent without too much effort, after which you must stop processing their personal information.
- ✓ **Specific:** The POPIA consent must clearly set out the specific purpose for which the personal information is processed. This means that the consent must relate to a specific defined study; simply obtaining consent to 'conduct research' will not be sufficient. Read section 3.4.2 on when you can do further processing of old data.
- ✓ **Informed:** Tell research participants
 - who the researchers are that will rely on the POPIA consent (you and any joint responsible parties);
 - why they are being asked for POPIA consent;
 - what personal information will be collected and used;
 - how to withdraw POPIA consent; and
 - whether any decisions will be made about the research participant.

The POPIA consent must be in [plain language](#). This means that the language must be appropriate for the intended research participants.

- ✓ **Explicit:** The POPIA consent must be given through a clear, unambiguous, and affirmative act. It cannot be provided by default, hidden, or deemed

from research participant's silence. It should be explicit, in writing or another recorded format. You must maintain a record of POPIA consents obtained from research participants during the research and for as long as identifiable personal information relating to that research participant is retained.



NB: The research participant has the right to withdraw their consent.

3.3.2. The research is required by law

If you are explicitly required to conduct research with an obligation imposed by law, POPIA consent is not required and the research participant will not have the right to object to the processing.



When will this apply?

The research must be necessary to comply with the obligation. In other words, the law must require that identifiable personal information must be processed before you can rely on this justification.

NB: If you want to rely on this justification, you must ensure that:



- ✓ you identify the specific law you are relying on;
- ✓ the processing is necessary to comply with the legal obligation;
- ✓ there is no less invasive way to comply with the legal obligation; and
- ✓ you document the decision to rely on this justification.

3.3.3. The research is conducted by a public body performing public law duty

You can rely on this justification if you are conducting research on behalf of a public body performing a public law duty.



What is a public body?

According to POPIA, a public body includes:

- any department of state or administration in the national or provincial sphere of government;
- any municipality in the local sphere of government;
- any other function or institution that is exercising power or performing a duty in terms of the Constitution or a provincial institution; and

- any other function or institution that is exercising public power or performing a public function in terms of any legislation.

Research participants will have the right to object to the research based on their situation. If a research participant objects, you must stop processing their personal information.

3.3.4. The research is in your legitimate interest or that of a third party

If you or a third party stands to benefit from the research, you can rely on this legitimate interest to justify the processing of personal information if the limitation on the privacy of the research participants is reasonable.²

The legitimate interest of the responsible party or third party must be weighed against the rights and interests of the data subject to make sure that there is no disproportionate infringement of privacy. You must show that the limitation of the research participant's right to privacy is reasonable.



What is a legitimate interest assessment?

A legitimate interest assessment has three steps:

- **Identify the legitimate interest:** What are the benefits to you, the third party or the research participant? Are there any wider public benefits? How significant are these benefits? What would be the impact if the research couldn't go ahead? Has the research received ethics approval?
- **Apply the necessity test:** Is it necessary to process the personal information to further your or a third party's legitimate interest? Is there another less intrusive way to achieve the same results?
- **Apply a balancing test:** Does the impact on research participants override your and third parties' legitimate interest? Is any of the personal information particularly sensitive or private? Are the research participants vulnerable? Would research participants expect their personal information to be processed this way? Will the processing be explained to them? Are research participants likely to object to the research or find it intrusive? What is the possible impact on the

² See the discussion on reasonableness on page 16 of the SA Law Reform Commission Project 124 on Privacy and Data Protection (2009 Report). Section 44(1)(b) of POPIA. See the Article 29 Data Protection Working Party Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, last accessed on 31 March 2022.

research participant? Can you adopt safeguards to minimise the impact?

See the Information Commissioner's Office [How do we apply legitimate interest in practice](#) for guidance.

Research participants will have a right to object to the research based on their situation. If a research participant objects, you must stop processing their personal information.



NB: You cannot rely on this justification if you are processing special personal information or the personal information of children.

3.3.5. When your research includes special personal information



Section 26 - Prohibition on processing of special personal information
Section 27 - General authorisations concerning special personal information

The standard position is that you are not allowed to process special personal information. However, POPIA provides a list of general authorisations for the processing of special personal information:

- **You will obtain the research participant's POPIA consent**
The same guidance as discussed above will apply.
- **The research is necessary for the establishment, exercise or defence of a right or obligation in law**
This authorisation allows you to process special personal information where it is necessary to exercise a right or claim it has in terms of South African law.
- **The research is necessary to comply with an obligation of international public law**
Public international law has three main sources, namely customary international law, treaties, and conventions.
- **The research is in the public interest**
What constitutes public interest varies across jurisdictions and should be assessed on a case-by-case basis. Research is in the public interest if the research process or outcome widely and generally benefits the public at large or a group,

community, or specific population (as opposed to a few individuals or a single entity).³

- **It is impossible or would require a disproportionate effort to get POPIA consent**
POPIA consent is not required if obtaining it is impossible or would require a disproportionate effort. However, given the inherent sensitivity of special personal information, it must be virtually impossible, as opposed to merely impractical or costly, to obtain POPIA consent before this legal justification applies.⁴
- **The research participant has deliberately made the personal information public**
For this legal justification to apply, the following requirements must be met:
 - ✓ **The personal information must have been made public:** There must be no impediment (for example, a paywall or a data wall) to the accessibility of the personal information.⁵
 - ✓ **By the research participant:** If someone else published the personal information, this legal justification does not apply. You must be able to prove who published the personal information.
 - ✓ **Deliberately:** There must be evidence of an unmistakably deliberate and affirmative action by the research participant.

3.3.6. When your research includes personal information of a child



Section 34 - Prohibition on processing of personal information of children
Section 35 - General authorisation concerning personal information of children



NB: You are responsible for verifying the age of research participants to ensure that you apply the correct legal justifications. For instance, you cannot use 'legitimate interest' as a legal justification to process the personal information of a child. When you verify the age of the research participant, you should not process more information than necessary to determine their age, and the processing must be proportionate to the nature and risks involved in the research.

³ Information Regulator *Guidance Note on Processing of Special Personal Information*, available at <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628.pdf> (last accessed on 30 March 2022).

⁴ This interpretation is consistent with how similar provisions have been interpreted in the courts in the EU and New Zealand.

⁵ This interpretation is based on how similar provisions in the New Zealand Privacy Act of 1999 has been interpreted. See Case Note 100413 [2007] NZ PrivCr 20, available at <https://www.privacy.org.nz/publications/case-notes-and-court-decisions/case-note-100413-2007-nz-privcmr-20-google-search-reveals-personal-information-on-law-firm-website/> (last accessed on 31 March 2022).

- **The research participant's parent or guardian (competent person), is asked for POPIA consent on behalf of the child**

If you want to rely on POPIA consent to justify the processing of personal information, you must obtain the POPIA consent from a 'competent person'. In terms of POPIA, this will be a person with parental responsibilities in terms of the Children's Act 38 of 2005. The same guidance regarding asking for consent discussed in section 3.6.1 applies.

A parent or legal guardian is a competent person who can provide consent on behalf of a child. The High Court of South Africa is the upper guardian of all children. For children who do not have parents or a legal guardian, the court will step in and fulfil that role.

You must make sure that the person who provides consent is the parent or legal guardian of the child and you must have measures in place to verify this. What measures are reasonable may depend on the risks inherent in the processing as well as the available technology. In low-risk cases, you could verify this via email and in high-risk cases it would be appropriate for you to ask for more proof.

When you rely on the consent of a competent person and the child becomes an adult, you must obtain new consent from the child once they have become an adult to continue processing their personal information.



A **competent person** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

- **The research is necessary for the establishment, exercise, or defence of a right or obligation in law**

This authorisation allows you to process special personal information where it is necessary to exercise a right or claim it has in terms of South African law.

- **The research is necessary to comply with an obligation of international public law**

Public international law has three main sources, namely customary international law, treaties, and conventions.

- **The research is in the public interest AND you can provide sufficient guarantees that the processing does not adversely affect the individual privacy of the child to a disproportionate extent**

What constitutes public interest varies across jurisdictions and should be assessed on a case-by-case basis. Research is in the public interest if the research process or outcome widely and generally benefits the public at large or a group,

community, or specific population (as opposed to a few individuals or a single entity).⁶

- **It is impossible, or would require a disproportionate effort to get POPIA consent AND you can provide sufficient guarantees that the processing does not adversely affect the individual privacy of the child to a disproportionate extent**
POPIA consent is not required if it would be impossible, or it would require a disproportionate effort to obtain it. Given the inherent vulnerability of children, it must be virtually impossible, and not just impractical or costly, to obtain POPIA consent before this legal justification applies.⁷

- **The child has made the personal information public deliberately with the POPIA consent of a competent person**

For this justification to apply, the following requirements must be met:

- ✓ **The personal information must have been made public:** There must be no impediment (for example, a paywall or a data wall) to the accessibility of the personal information.⁸
- ✓ **By the child:** If someone else published the personal information, this legal justification does not apply. You must be able to prove who published the personal information.
- ✓ **Deliberately:** There must be evidence of an unmistakably deliberate and affirmative action by the child.
- ✓ **With the POPIA consent of a competent person:** Someone with parental responsibility must have consented to the disclosure made by the child.

3.4. Sourcing the personal information



Section 12 - Collection directly from a data subject

When you define the purpose of your research, you must record how you will collect personal information and what you will do with it.

⁶ Information Regulator *Guidance Note on Processing of Special Personal Information*, available at <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628.pdf> (last accessed on 30 March 2022).

⁷ This interpretation is consistent with how similar provisions have been interpreted in the courts in the EU and New Zealand.

⁸ This interpretation is based on how similar provisions in the New Zealand Privacy Act of 1999 has been interpreted. See Case Note 100413 [2007] NZ PrivCr 20, available at <https://www.privacy.org.nz/publications/case-notes-and-court-decisions/case-note-100413-2007-nz-privcmr-20-google-search-reveals-personal-information-on-law-firm-website/> (last accessed on 31 March 2022).

3.4.1. The direct collection rule

According to POPIA, you must keep a record of where the personal information was collected. Ideally, personal information should be collected directly from the research participants. Collecting personal information from other sources is not recommended, as the research participant may be unaware of the data collection, and the other sources may not always be reliable.

Only in the following circumstances can you collect personal information from other sources:

- **The personal information is available in or derived from a public record**



What is a public record?

A public record is:

- accessible to the public domain: If there is restricted access (for example, a paywall, a data wall, or a data access committee), the personal information is not in the public domain. An open-access repository is not in the public domain, because there will generally be some access restrictions.
- in the possession of or under the control of a public body: A public body is a national or provincial department, municipality or local government, an institution which gets its mandate from the South African Constitution or a provincial constitution or an organisation that exercises a public function.



NB: The internet or a social media platform is not a public record.

- **The research participant made the personal information public deliberately**
You will have to prove that the research participant made the personal information public themselves or consented that someone else made the personal information public intentionally. Although this will sometimes be the case with personal information published on the internet, it is not always the case.
- **The research participant consented (more on that in section 3.6.1) to their personal information being collected from another source**
This POPIA consent must meet the requirements of legal justification discussed in section **Error! Reference source not found.** It is not sufficient to obtain a blanket POPIA consent to collect personal information from 'other sources'. The POPIA consent should contain a list of the sources that will be used.

- **Collecting the information from another source does not prejudice a legitimate interest of the data subject**

You should document the positive and negative impacts of collecting personal information from another source. If the positive implications outweigh the negative repercussions, collecting personal information from another source is justified.

- **Collecting personal information from another source is needed to maintain the legitimate interest of the responsible party, or a third party to whom the information is supplied**

If you want to argue that collecting personal information is needed to maintain your legitimate interest or that of a third party, you must include this reasoning in your legitimate interest assessment.

- **Collecting personal information directly from the research participant would prejudice the lawful purpose of the research**

In some instances, it may be detrimental to the research if the personal information is (only) collected directly from the research participants, for example, if there are strong reasons to believe that research participants will not be truthful or do not have access to reliable personal information (for example, reliable location or behavioural information). You must document why collecting the personal information directly from the research participant will undermine the study.

- **It is not 'reasonably practicable' to collect the personal information directly from the research participant**

You can rely on this exception if it would be virtually impossible to obtain personal information directly from the research participants, for example, if you do not have the contact details of research participants and have no way to get the contact details. However, if it would be very difficult and expensive to contact research participants, then you cannot rely on this exception. In other cases, research participants may not have personal information about themselves (for example, accurate location or behavioural information).

3.4.2. Using previously collected data for new purposes

In some cases, you might not want to collect new personal information but rather use previously collected data previously collected for another purpose. In POPIA, this is called "**further processing**". POPIA allows you to do further processing without getting new POPIA consent, if the new reason for using the personal information is compatible with the purpose for which it was collected.



What does POPIA say?

Although section 15(3) gives a couple of justifications for further processing, the most common justification for further processing for research purposes will

be section 15(3)(e). Section 15(3)(e) provides that the reuse of personal information for research purposes will be allowed without obtaining POPIA consent if:

- the personal information will only be used for research purposes; and
- the personal information will not be published in an identifiable form.

If you want to do further processing of special personal information or the personal information of a child, you must also abide by sections 27(1) and 35(1). The most common justifications for further processing of special personal information or the personal information of a child are sections 27(1)(d) or 35(1)(d). These sections indicate that further processing of special personal information or the personal information of a child is authorised without obtaining POPIA consent if:

- the research serves a public interest, and the processing is necessary for that purpose; or
- it would be impossible or would involve a disproportionate effort to ask for POPIA consent; and
- you can provide sufficient guarantees that the processing does not adversely affect the privacy of the research participant to a disproportionate extent.

If you cannot use these justifications for further processing, then you need to get POPIA consent to reuse the personal information that you previously collected. More on POPIA consent in section 3.5.



NB: Even if POPIA allows you to do further processing without getting POPIA consent again, you still need to comply with the rest of POPIA in your new research.

If you want to use previously collected personal information for a completely different purpose, you must provide the following information in the new research document:

- ✓ the circumstances under which the personal information was initially collected (including what was disclosed to research participants and information about any POPIA consent that was obtained);
- ✓ how you will ensure that the personal information will only be used for research purposes and that it will not be published in an identifiable form (for example, contractual undertakings or that there will be a data access committee or both);
- ✓ how you will comply with the notification requirements (more on that in section 3.6.2); and
- ✓ if the data was not collected by you, whether you have permission from the previous researcher who initially processed the personal information.

3.4.3. Minimal processing

You must make sure that the personal information that you process is absolutely necessary for your research.



What does POPIA say?

Section 10 says that personal information may only be used in research if, given the purpose of the research, the personal information is adequate, relevant, and not excessive.

You must ensure that the processing of identifiable personal information is necessary and proportional.⁹ Use these questions to determine whether that is the case:

- **Is it necessary to collect all the personal information?**
You should only collect personal information that is necessary to achieve the purpose of the research. You cannot collect personal information just in case you might use it in the future, but it is still possible to collect personal information for possible foreseeable future use that you (or future researchers) will require. If this is the case, you must document potential future uses as accurately as possible.¹⁰
- **Is there a less intrusive way to process the personal information?**
You must determine the least intrusive way to process personal information, for example, [pseudonymisation](#).



What is pseudonymisation?

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

Want to learn more about pseudonymisation? Read these documents:

⁹ The question is whether the processing is a justifiable limitation of the research participant's constitutional right to privacy (see section 36(1) of the Constitution). This is determined by assessing whether the processing is necessary and proportional. This test is consistent with the approach taken in the EU when conducting data protection impact assessments. See also ICO 'How do we do a DPIA?', available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/> (last accessed on 31 March 2022).

¹⁰ See ICO 'Data Minimisation', <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/> available at (last accessed 9 September 2024).

- [ICO 'Draft anonymisation, pseudonymisation and privacy-enhancing technologies guidance: Chapter 2'](#)
- [Irish Data Protection Commission' Guidance on Anonymisation and Pseudonymisation'](#)

In high-risk research, you must pseudonymise personal information to limit the number of people who have access to research participants' identities. If pseudonymisation is not possible, you must document why. If you share personal information with third parties, it must be pseudonymised and the agreement between you and the third party must prohibit re-identification.

3.5. Asking for POPIA consent

You may also have to obtain consent to process research participants' personal information, depending on the reason for the processing.

3.5.1. POPIA consent is different to research consent

It is important to note that there is a difference between POPIA consent and research or informed consent. When you apply for ethics clearance at your research institute, the ethics committee will ask that you create an informed consent form.¹¹ This form is given to research participants and explains what the research is about and the rights of research participants. If you ask for POPIA consent, that means that you ask research participants to give you permission to process their personal information. POPIA consent is usually asked in the research consent form, but in some instances, you do not have to ask for POPIA consent.

3.6. Contacting participants

Once you've indicated how you will ask for consent, you should establish how you will contact research participants.

3.6.1. Asking for consent

¹¹ It is essential to separate POPIA Consent from Research Consent (which may be required in terms of the National Health Act 61 of 2003 or to comply with ethical principles). While the content of these consents may overlap significantly, POPIA Consent is not always required. POPIA is very similar to the EU GDPR in this regard. See the European Data Protection Board EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health Research (https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaire_research_final.pdf) and the European Data Protection Supervisor A Preliminary Opinion on data protection and scientific research (https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf).

You should always ask for research consent before a research participant can take part in your research. Your institution's ethics committee will provide guidance on how to request [research consent](#).

You should ask for POPIA consent from the participant, unless you are planning to rely on another legal justification for processing personal information.



NB: You must make sure that the research participant can ask questions and that they completely understand the consent.

3.6.2. Transparency and notification



Section 18 - Notification to data subject when collecting personal information)

Section 18(4)(f)(ii) - Exception to the notification requirement

When you contact research participants you have to be transparent about the processing. You must notify data subjects of:

- the information being collected and the source from which the information is collected;
- the name and address of the responsible party (you or the institution);
- the purpose for which the information is being collected;
- whether the supply of the personal information by the data subject is voluntary or mandatory;
- the consequences if they fail to provide the information;
- any particular law authorising or requiring the collection of the information;
- your intent to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;
- any other information such as:
 - the recipients or category of recipients;
 - the nature or category of the personal information;
 - the existence of the research participant's rights; and

the contact details of the Information Regulator. POPIA does provide an exception to the notification requirement if you are processing personal information for historical

statistical or research purposes. However, you should provide this information even though POPIA does not legally require you to do so.

3.6.3. Participants' rights



Section 5 – Rights of data subject
Section 11 – Consent justification and objection
Section 23 – Data subject participation
Section 24 – Correction of personal information
Section 25 – Manner of access
Section 71 – Automated decision making

The **Promotion of Access to Information Act** is also relevant:

Section 30 – Access to health or other records
Section 34 – Mandatory protection of privacy of third party who is a natural person
Section 61- Access to health or other records
Section 63 - Mandatory protection of privacy of third party who is a natural person

When you contact research participants, you must ensure that they have the opportunity to exercise their POPIA rights. This process must be effortless and free.

Research participants have the following rights:

- **The right to object to processing on reasonable grounds relating to their situation**
Research participants have the right to object to the processing of their personal information on reasonable grounds related to their situation if you rely on any one of these legal bases, namely that the:
 - processing is protecting a legitimate interest of a research participant;
 - processing is necessary for the proper performance of a public law duty by a public body; or
 - processing is necessary to pursue your legitimate interests or that of a third party to whom the information is supplied.

The POPIA Regulations prescribe a form that research participants may use to object.¹² Once the research participant has objected and if it was found that the objection was reasonable, you must stop processing the personal information, unless processing is justified by legislation.

¹² Form 1 available at: <https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-1-OBJECTION-TO-THE-PROCESSING-OF-PERSONAL-INFORMATION.pdf>

- **The right to make representations about automated decisions with a legal or substantial effect**

Research participants have additional rights if the research involves automated decision-making.



What are automated decisions?

Automated decisions are decisions that:

- have legal consequences or will have a substantial effect on the research participant (for example, if they will receive medical treatment or not);
- are automated (i.e., made without human intervention); and
- are based on an analysis of aspects of a research participant's personality, behaviour, interests, and habits (for example, performance at work, creditworthiness, reliability, location, health, personal preferences, or conduct).

When research involves automated decision-making, you must:

- ✓ give research participants an opportunity to make representations about that decision; and
- ✓ provide research participants with sufficient information about the underlying logic of the automated decision to allow research participants to make representations to you about the decision.

- **The right to access their own personal information**

Research participants have the right to access their personal information, or to request a copy of what personal information is being used in research.

This right is not absolute. For instance, they are not entitled to their own personal information if giving access would:

- reveal the personal information of someone else without their permission;
- cause serious harm to the research participant's physical or mental health, and the research participant has not arranged for counselling;
- expose the research to serious disadvantage; or
- compromise someone else's intellectual property or confidential information.

- **The right to correct or delete their personal information**

Research participants can ask that you correct personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, or misleading.

If you receive such a request, you must either:

- ✓ correct or delete the personal information; or

- ✓ provide credible evidence that the research participant is satisfied that the personal information is correct. In the interim, the personal information must be restricted.

If you and the research participant cannot agree on the accuracy of the personal information, you must indicate in your records that there is a dispute about the accuracy of the personal information.

If you agree that the personal information should be corrected or deleted, and if this change affects the decisions that have been or will be made regarding the research participants, you must inform everyone to whom the personal information was shared about the correction or deletion.

3.7. Collecting data

Once you've properly informed the research participant about your research and its purpose and their POPIA rights, you can start to collect your data.

3.7.1. Adhere to your research document

It is important that once you start collecting your data that you adhere to the plan set out in your approved research document. If you start collecting data and you realise that the plan in your research document does not work in practise or that you need to make changes, you must update your research document and resubmit it for approval.

3.7.2. Information quality



Section 16 – Quality of information

When you collect data, the information must be of high quality. You must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading, and updated where necessary.

Follow these guidelines to make sure that you collect high-quality personal information.

- **Use reliable sources**

If you collect personal information from sources other than the research participant, you must put additional safeguards in place to guarantee the reliability of the personal information. This could include:

- ✓ verifying the personal information of the research participants;
- ✓ using multiple sources to verify the personal information; or
- ✓ obtaining contractual guarantees regarding the accuracy of the personal information.

You must maintain a record of the source of all personal information.

- **Data quality reviews**

You must document data quality reviews in your research documents to ensure that the personal information you collect is complete, accurate, not misleading,

and updated where necessary. The frequency of data quality reviews will depend on the type of personal information you collect, how quickly it will age, and the potential harm it could cause to research participants if the information is incorrect. For example, ID numbers do not change often, so regular data quality reviews are not necessary. You must document in your research document that data quality reviews were considered and document the reasons for your approach.

- **Provide research participants with access**

Research participants have the right to access their own personal information. Even though this right is not absolute, research participants should have effective access to their personal information and correct it if necessary. If effective access is impractical or would harm the research participant, you should document the reasons for not granting access by default in your research document.

- **Data management**

The quality of personal information should be managed centrally. If you allow for copies, it must be for specific and documented reasons with strict version control.

- **Techniques to minimise the risk of error or discrimination (bias)**

This is particularly important if the research involves profiling research participants and making automated decisions about them. The risk of error or bias increases when big data is used in research along with artificial intelligence and machine learning technologies. If the automated decision has a legal or otherwise significant impact on the research participant, you must:

- ✓ understand the technology and algorithms;
- ✓ provide research participants with sufficient information about the underlying logic of the automated decision;
- ✓ understand preferences or biases that may exist and identify risks to research participants;
- ✓ monitor and review the automated decisions for discrimination or bias; and
- ✓ ensure that research participants have an opportunity to make representation about the outcome of the automated decision.

3.8. Storing data



Section 14 – Retention and restriction of records

Once you've collected your data, including personal information, it must keep it safe. While your research institution will have procedures in place, you also have the responsibility to ensure the safety of the data.

3.8.1. Retention and restriction of records

You must document how research records will be retained in your research documentation, referred to as a “**retention record**”. Your retention record must balance the principle of minimal processing, as discussed in section 3.4.3, and the research institution’s needs to preserve an authoritative record of its research activities. Your research institution will give you guidance on how to retain your records safely according to its procedures.

You must keep records of the following types of research-related activities:

Research administration information

Documents and information relating to the administration of the research, including:

- ✓ research documents
- ✓ research ethics approval applications
- ✓ correspondence between you and approval bodies (for example feedback from research ethics committees or advice from deputy information officers)
- ✓ research-related contracts
- ✓ disclosures made to research participants (for example information sheets)
- ✓ POPIA consent or research consent, or both, provided by research participants (including the procedure and documentation used)
- ✓ Progress or other reports

Identifiable personal information of research participants

All identifiable personal information of research participants must be de-identified as soon as possible. If there is a persuasive reason why it cannot be de-identified, you must record the following:

- ✓ the source of the personal information
- ✓ who accessed the personal information
- ✓ who made changes to the personal information, when and why
- ✓ how long the information must be retained (including the start date)
- ✓ what disclosures were made to the research participant (including a reference to the notification document)
- ✓ whether the research participant provided a POPIA consent (including a reference to the consent documentation)
- ✓ under which conditions the personal information can be shared with external institutions or researchers
- ✓ what the personal information can be reused for in the future

De-identified research data

You must keep a record of any personal information that you collected from research participants that are no longer identifiable by keeping a log that contains the following metadata:

- ✓ when the personal information was de-identified
- ✓ how the personal information was de-identified

- ✓ under which conditions it can be shared on open-access platforms

3.9. Sharing personal information

Sometimes you will have to share the personal information that you collected with other people, such as operators or collaborators. According to POPIA, there are specific requirements you must follow when sharing personal information.

3.9.1. How to assess whether you can share personal information

You must ensure that your data sharing complies with all conditions for the lawful processing of personal information, which requires conducting a Personal Information Impact Assessment (PIIA).

You need to:

- determine what personal information is shared;
- determine and document the purpose for sharing the personal information;
- identify who is accountable for POPIA compliance;
- assess whether you need prior authorisation from the Information Regulator to share;
- determine whether personal information will travel across borders and assess the level of protection provided outside of South Africa;
- identify the legal basis for sharing;
- confirm that an exemption to the direct collection rule applies;
- assess whether the notification requirements have been met;
- assess whether sharing complies with the principle of minimal processing;
- assess whether the means of sharing is secure; and
- determine whether the person (or institution) you are giving the information can honour the rights of your research participants.

3.9.2. Sharing personal information with operators

POPIA requires that there must be a written agreement between the responsible party and their operator. This must state that the responsible party will ensure that the operator establishes and maintains appropriate technical and organisational security measures.

**NB:**

Your operator agreement should:

- Identify the Information Officers;
- describe the purposes for which the operator may process personal information;
- limit the purposes for which the operator may use the personal information to instances you have authorised the operator;
- demand that the operator must keep the personal information confidential and not share it with third parties without your written approval;
- reserve the right that you can demand the return or destruction of personal information;
- describe how the operator must deal with requests and complaints from a data subject, or notices, requests and complaints from the Regulator;
- describe the information and cyber security measures that the operator must have in place;
- describe the process that the operator must follow when they experience a security compromise;
- include obligations, if the operator is situated outside South Africa, to ensure the operator provides an adequate level of protection that effectively upholds the principles for the reasonable processing of the information that are substantially similar to the principles of POPIA;
- include a right to audit the operator's compliance with POPIA and the security requirements, when appropriate; and
- consider whether indemnities and limitations of liability is appropriate.

3.9.3. Sharing personal information with other responsible parties

You must sign a personal information sharing agreement that contains a common set of rules followed by all parties involved.

**NB:**

Your personal information sharing agreement (which can also be called a data sharing agreement, data use agreement, data transfer agreement or material transfer agreement) should contain:

- who the Information Officer of each party is;
- what the purposes are for sharing the personal information;
- if the use of the personal information is limited to the purposes for which it was shared in the first place;
- that the parties must keep the personal information confidential;
- whether the institution may demand the return or destruction of the personal information held by third parties;
- how the parties will manage requests and complaints from the data subjects, or requests from the Regulator;
- what information and cybersecurity measures each of the parties must have in place;
- a procedure to give notice and manage an information security compromise;
- the applicable data protection regulations and undertakings by foreign third parties to effectively uphold the principles for the lawful processing of personal information outside South Africa;
- the responsibilities of the parties to notify research participants;
- the obligations to maintain the quality of information;
- what appropriate indemnifications there are; and
- for how long the agreement will remain and what must happen with the personal information after the contract has come to an end.

3.9.4. Transborder information flows



Section 72 – Transfers of personal information outside the Republic

Research activities often require the transfer of personal information to other countries. You must document all transborder information flows, and the transfer must meet one of the following requirements:

- If the recipient of the personal information is a collaborator (a joint responsible party), you must conclude an agreement (such as a data transfer agreement¹³) with them to ensure their compliance with this framework.
- If the recipient is an operator, you must conclude an agreement with them to ensure their compliance with the security safeguards that your research institution put in place.
- The research participant consents to the transfer of personal information. There must also be a process in place to allow the withdrawal of POPIA consent.
- The third party is subject to a law binding corporate rules, or a binding agreement that provides an adequate level of protection. Protection will be 'adequate' if the law, rules, or agreement is 'effective' if it upholds principles for reasonable processing of personal information that are substantially similar to the principles in POPIA, and if it includes provisions about the further transfer to another third party in a foreign country that are substantially similar to POPIA.
- The transfer is necessary to conclude or perform in terms of a contract concluded in the interest of the research participant between you and the third party. The research participant will benefit from the transfer, but it was impossible to obtain their POPIA consent, and they would likely have consented if asked.



What does POPIA say?


POPIA allows for the cross-border transfer of personal information if the recipient of the information is "subject to a law ... which provide[s] an adequate level of protection". Although you are not equipped to determine if the law provides an adequate level of protection, your research institution and ASSAf will be able to assess the adequacy of the law.

Binding corporate rules means personal information processing policies within a group of undertakings that must be adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country.

A group of undertakings means a controlling undertaking and its controlled undertakings

3.10. Publishing data for further processing

¹³ See *A data transfer agreement template for South Africa* by Lee Swales et al for a DTA template and explanatory memorandum (https://zenodo.org/record/7537396#.Y_b74-xBzAN).



In some cases, you might want to publish your data or the journal where you publish your data requires that you give other researchers access to your data.

3.10.1. Using previously collected data for new purposes

In section 3.4.2, we discussed when further processing is allowed. These guidelines also apply when you intend to publish your data.

4. POPIA COMPLIANCE FOR INSTITUTIONS AND INDEPENDENT RESEARCHERS

If you are a research institution or an independent researcher, you need to put certain procedures in place to comply with POPIA.



NB: Are you an independent researcher?

If you are a researcher who does not work under a research institution, you are therefore the sole responsible party. That means that you must put the following procedures in place yourself.

4.1. Your responsibilities

To comply with POPIA, research institutions and independent researchers must:

- ✓ monitor and comply with this framework;
- ✓ create an accountability checklist;
- ✓ implement a Personal Information Impact Assessment;
- ✓ put appropriate safeguards in place;
- ✓ act on security compromises; and
- ✓ put structures in place for retaining records.

These responsibilities are discussed in detail in the rest of this section.

4.2. Monitoring and compliance with the framework

You must show that you comply with this framework. ASSAf may, on its own accord, or in response to a complaint:

- ask you to demonstrate that you comply with the framework by producing documentation discussed in the next section; or
- require that you produce a report by an independent auditor that you comply with the framework at your own cost.

4.3. Accountability checklist

You must perform the following tasks to comply with the requirements in POPIA regarding accountability (condition 1) and openness (condition 6).

- ✓ **Appoint an Information Officer and a Deputy Information Officer** (where the size of your institution justifies it) who must ensure compliance with the framework. The Information Officer or Deputy Information Officer's role description must be stated in writing and must explicitly refer to the framework. If you are a foreign institution, you must appoint a Deputy Information Officer in South Africa. See the

Information Regulator's Guidance Note on Information Officers and Deputy Information Officers for further guidance.

- ✓ **Create a POPIA compliance framework.** This framework must document how the framework will be implemented in your policies, procedures, standards, templates, and other binding documents. These documents must set out the responsibilities of different research-related roles, including research management (for example, directors responsible for research activities), research ethics committees and other approval bodies, lead researchers (for example, principal investigators, study leaders, supervisors), and other researchers. At least once every five years, the Information Officer and Deputy Information Officer must review these documents and audit your compliance.
- ✓ **Have a Promotion of Access to Information (PAIA) manual that contains a general description of:**
 - ✓ **The type of research you conduct:** the PAIA manual must contain general information about your research activities. It is not necessary to list all research activities.
 - ✓ **Different types of research participants:** For example: the public, employees, clients, or students.
 - ✓ **The different categories of personal information used in research:** For example: health information, financial information, political views, and contact details. List any special personal information.
 - ✓ **Categories of third parties with whom personal information will be shared:** For example: information technology service providers, open-access platforms and collaborators.
 - ✓ **Planned transborder information flows:** Some third parties may be in other countries. You should list all significant planned transborder information flows.
 - ✓ **The security measures implemented to protect personal information:** You should indicate that you comply with this framework and include a link to it.
 - ✓ **How to exercise POPIA rights:** The PAIA manual must contain a detailed description of the procedures that research participants must follow to exercise their POPIA rights.

See the Information Regulator's PAIA manual templates for guidance on PAIA manuals.

- ✓ **Include a documented research PIIA (Personal Information Impact Assessment) in its processes.** You may decide who is responsible for ensuring that a research PIIA is performed, but the assessment must be done before the research starts. More on PIIA in the next section.
- ✓ **Ensure that everybody involved in research-related activities receives training on their data protection responsibilities.**
- ✓ **Assess compliance with the framework** and binding documents periodically.

4.4. A three-phase research PIIA

All researchers conducting research at your research institution must go through a PIIA to ensure that you manage the risk to research participants appropriately by including appropriate safeguards.¹⁴

This framework prescribes a three-phase research PIIA:

- **Phase 1:** Inherent risk assessment to determine whether the research should be classified as high-risk.
- **Phase 2:** Self-assessment to determine whether the research document complies with POPIA.
- **Phase 3:** Implementation and monitoring to record security safeguards and a monitoring plan in the research document.



NB: It is your responsibility to make sure that researchers perform a PIIA for each research activity (for example a project or study).

To ensure that the framework does not hinder research, it permits self-assessment by researchers. Information Officers, Deputy Information Officers, or a senior employee formally designated to perform this task on their behalf (such as members of Research Ethics Committees) must incorporate the research PIIA in their policies, procedures, or other binding rules. They are also required to conduct annual reviews of selected high-risk research activities to evaluate the level of compliance. The level of additional oversight or approval is left to your discretion.

4.4.1. Inherent risk assessment

The inherent risk assessment determines how actively you must monitor whether a project is POPIA compliant. The inherent risk assessment aims to identify high-risk research and encourages researchers to re-evaluate whether their research warrants high-risk practices and to include safeguards in their research documents to mitigate the inherent risk.

You must include the following questions in the inherent risk assessment.¹⁵ If any of the answers are “Yes”, the research will be considered inherently high-risk.

- ✓ **Will the research include children or special personal information?**

¹⁴ Regulation 4(1)(a) of the POPIA regulations provides that Information Officers must perform Personal Information impact assessments (PIIAs). POPIA does not prescribe how PIIAs must be performed.

¹⁵ The questions are a combination of what is considered high-risk in terms of article 35 of the GDPR and the types of Research that would have required prior authorisation in terms of section 57 of POPIA.

The personal information of children is subject to additional protection. Provide researchers with a checklist of special personal information because special personal information is subject to additional protection.

✓ **Will the research involve processing personal information on a large scale?**

Processing is considered on a large scale if:

- many research participants are involved;
- a large proportion of the population is involved;
- a large volume of personal information will be collected (even if there are only a few research participants); or
- the processing will take place over a long period (for example, longer than the average research activity).

✓ **Will the research involve the evaluation or scoring of personal information to make automated decisions with legal consequences or that have a significant effect on research participants?**

This includes research that uses profiling and predictive analysis (such as cardiovascular disease risk calculations) to make an automated decision about the research participant that will have a significant effect on the research participant. A decision is automated if there is no human involvement in the decision. For the answer to be “yes”, the automated decision must affect the research participant’s circumstances, behaviour, or choices. It might affect their financial status, health, reputation, access to services, or other economic or social opportunities. If the decision is trivial or hypothetical and has no real effect, the answer to this question should be “no”.

✓ **Will the research involve processing where the researchers are getting research participants’ personal information from sources other than the research participant themselves?**

Typically, this will happen when research participants’ personal information is collected from another source (such as the internet, social media platforms, the research participants’ employer, or organisations that render services to the research participant).

✓ **Will the personal information of research participants be disclosed to third parties?**

This will happen if personal information is transmitted to another organisation or person, or if they are given access to the personal information.

✓ **Are any people or organisations that will have access to the personal information located in another country?**

This will happen if personal information is transmitted to another country or an organisation or person in another country is allowed to access the personal information.

✓ **Will unique identifiers be used to link, combine, compare, or match personal information from multiple sources?**

This will happen if different sets of personal information held by other organisations or persons are linked by using unique identifiers to form a new dataset.



What are unique identifiers?

A unique identifier is a code or a number that an organisation uses to identify a research participant. This would include an ID number, participant identification number, sample code, requisition number, or another reference number that identifies a research participant.

- ✓ **Does the research involve the use of new technology or technology that is, or might be, perceived by individuals as intrusive on their privacy?**
Examples include artificial intelligence, machine learning, deep learning, smart or wearable technology, neuro-measurement (emotional response analysis and brain activity measurement), tracking technology, or the use of biometric information.
- ✓ **Will the processing of personal information contemplated by the researchers be outside of the reasonable expectations of the research participants?**
Will research participants be surprised to learn what their personal information will be used for, or how it will be used, or will they find it invasive?
- ✓ **Will the research involve contacting or interacting with research participants in ways they might find intrusive?**
This will happen for instance, when personal information is collected by systematically monitoring the research participants in publicly accessible places without their knowledge.

If the researcher answered “yes” to any of these questions and the research activity is therefore high-risk, an Information Officer, Deputy Information Officer, or a senior employee formally designated to perform this task on the researcher's behalf (such as a member of the research ethics committee or another committee or individual) must:

- ✓ confirm whether the researcher performed the self-assessment;
- ✓ ask researchers to confirm periodically that they have implemented the research document; and
- ✓ ensure that the personal information is pseudonymised unless there is a compelling reason why it is not feasible or appropriate.



NB: Regardless of the outcomes, you must keep a record of the inherent risk assessment.

4.4.2. Perform a self-assessment

After researchers have performed an inherent risk assessment, they must perform a self-assessment against the eight conditions of lawful processing according to POPIA. This will help them to determine where there is room for improvement or whether safeguards should be implemented. These eight conditions are discussed in the previous section, and they are:

- Processing limitations
- Purpose specification
- Further processing limitation
- Information quality
- Openness and notification
- Security safeguards
- Research participant participation

4.4.3. Implementation and monitoring

Researchers performing high-risk research must complete an annual declaration confirming that the self-assessment they have conducted is still valid (i.e., that the way they process personal information has not changed) and that they are implementing the safeguards prescribed by their research document.

Information Officers, Deputy Information Officers, or a senior employee formally designated to perform this task on their behalf (such as a member of the research ethics committees) must perform annual reviews of selected high-risk research activities to evaluate the levels of compliance. The level of additional oversight or approval by Information Officers, Deputy Information Officers, or a senior employee is left to your discretion.

4.5. Appropriate technical and organisational safeguards

You must establish appropriate technical and organisational safeguards. When considering what is appropriate, you may set different requirements depending on the outcome of the risk assessment. You must also obtain expert advice on how to achieve the level of security that is proportionate to the risk faced by the research participants.

You must make sure that researchers document the specific technical and organisational safeguards that will be put in place in their research document.

You must put the following technical and organisational safeguards in place when feasible. If it is not possible to implement these safeguards, you must document the reason for non-implementation and outline the alternative technical and organisational

measures in place to ensure the integrity and confidentiality of the personal information.¹⁶

✓ **Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and software**

You must put the following safeguards in place:

- ✓ **Access control procedures and access logging:** You must have policies and procedures in place that regulate access to personal information used in research. You must apply the principles of “role-based access” (i.e., need to know) and “least privilege” (such as limited ability to modify personal information) in this procedure. You must ensure that researchers are identified before they are granted access to identifiable personal information. For access control, a one-factor authentication (for example, a strong password) is required, but two-factor authentication is recommended. If you did not implement a two-step authentication, you must document why it was not possible. You must document who has access to identifiable personal information and log any changes to the personal information.
- ✓ **Third-party risk management:** If you use operators, you must conclude a written agreement in which third parties undertake to comply with your safeguards or their equivalent.
- ✓ **Use of acceptable software:** You must have rules in place about what software is acceptable to be used in research and you must provide guidance to researchers on how to use that software securely. You must approve all software that researchers want to use in their research.
- ✓ **Storage security:** You must ensure that researchers store personal information in a way that prevents unauthorised access (for example, authentication and access control, use of passwords to access electronic files, local encrypted storage, and database encryption). You must ensure that these safeguards are applied to local computers, portable storage devices, and cloud-based computing services.
- ✓ **Security for transfers and communication:** You must ensure safe electronic communication for transferring personal information (for example, encrypted communication, secure file transfer protocols, Virtual Private Networks (VPNs), firewall systems, anti-virus, and anti-malware systems) and that personal information is protected when it is physically transferred.

¹⁶ These safeguards are aimed to ensure that a similar standard is maintained to the standard required in the EU. The sources of these safeguards are article 32 of the EU GDPR, European Data Protection Board *Guidelines 4/2019 on Article 25 Data Protection by Design and Default* from page 8

(https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf), the ICO commentary on security (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>), and the European Data Protection Supervisor *Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research: Final Report (EDPS/2019/02-08)* (https://edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf).

- ✓ **Mobile devices, home or remote working, and removable media:** You must have policies and procedures in place to manage security risks associated with the devices researchers use. You must put protection in place to avoid unauthorised access (for example, encryption and remote wiping capabilities). You must put security measures in place to protect personal information when researchers are working from home or working remotely (for example, VPN and two-factor authentication). Personal information may only be stored on removable media if it is necessary. You must implement a software solution that can set permissions or restrictions for individual devices as well as an entire class of devices and that will enable you to provide support and update devices remotely.
 - ✓ **Physical security:** You must secure areas that contain high-risk research by appropriate entry controls and sign-in procedures. You must make researchers aware that paper records containing personal information must be secure, and access must be controlled. You must implement a clean desk and clear screen policy where personal information is processed.
 - ✓ **Back-ups:** You must ensure that systems are resilient and backed up. You must make researchers aware that they must be able to restore access and availability to personal information in a timely manner in the event of a physical or technical incident.
-
- ✓ **Pseudonymisation**
Pseudonymisation must be the default for all high-risk research. Where high-risk research deviates from pseudonymisation, the researcher must document why. You must encourage pseudonymisation in all other research. Researchers must state when and how the personal information will be pseudonymised (for example before sharing the personal information or before publication) in their research documents. Personal information must be pseudonymised as soon as possible. You must provide guidance on acceptable pseudonymisation techniques.
 - ✓ **Encryption**
You should consider encryption for personal information that is not pseudonymised as the default for all high-risk research. Where researchers cannot encrypt the personal information that cannot be pseudonymised, their reasons must be documented. You should encourage encryption in all other research.
 - ✓ **Restricted environment for high-risk research**
If your researchers regularly engage in high-risk research, you are strongly encouraged to establish restricted environments where research can be stored and transferred. These restricted environments must be certified to the [ISO27001 Information Security Management](#) standard or other similar standards.

4.6. Security compromises



Section 22 - Notification of security compromises

You must implement an incident reporting and response procedure if there are reasonable grounds to believe that the personal information of research participants has been accessed or acquired by an unauthorised person.

The response procedure must include the following:

✓ **Establish an incident reporting procedure**

You must specify where and how incidents must be reported.

✓ **Mitigate risks immediately**

You must take steps to:

- ✓ mobilise security compromise response teams;
- ✓ notify law enforcement if there is criminal conduct;
- ✓ restore the confidentiality, integrity, and availability of the personal information or the information system;
- ✓ assess the scope of the compromise; and
- ✓ preserve evidence.

✓ **Conduct a risk assessment**

You must conduct a risk assessment to assess the risk posed to research participants. This includes assessing:

- ✓ the identity of the unauthorised person(s) and their possible motives;
- ✓ the possible consequences of the security compromise; and
- ✓ a description of measures that you or the researcher or research participants can take to mitigate the consequences.

✓ **Notify the Information Regulator and the researcher(s) of the suspected security compromise AND notify research participants**

You must, after completing the immediate risk mitigation and the risk assessment, send out the following notification as soon as reasonable after you discover the compromise.

The notification must include:

- ✓ the steps you took to immediately mitigate the risk;
- ✓ the outcome of the risk assessment;
- ✓ an outline of future steps to mitigate the risk caused by the security compromise; and
- ✓ a communication plan and the wording of messages to research participants.

You must send the breach notification to:

- ✓ The Information Regulator: POPIACompliance@inforegulator.org.za

Unless a public body in law enforcement or the Information Regulator asks for a delay, you must notify research participants of the security compromise as soon as reasonably possible after it is discovered.

The notification to research participants must comply with sections 22(4) and (5) of POPIA.



What does POPIA say?

Sections 22(4) and (5) of POPIA say that you must communicate the notification to research participants by:

- mailing it to their last known physical or postal address;
- e-mailing it to their last known e-mail address;
- placing it at a prominent place on your website;
- publishing it in the news media; or
- or any other way that the Information Regulator might direct.

The notification must give the following information:

- ✓ It must give a description of the possible consequences of the security compromise.
- ✓ It must give a description of what you intend to do or have done to address the security compromise.
- ✓ It must give a recommendation of what the research participant can do to protect themselves from the possible effects of the security compromise.
- ✓ If you know who has gotten access to the research participant's information, you must indicate who it is.

- ✓ **Report to the Information Regulator on measures to prevent future security compromises and agree on a monitoring plan**

The Information Regulator may require that you provide a report on measures to prevent future security compromises and may require that you provide progress reports to ASSAf or the Information Regulator.

You must also ensure that researchers and other staff are trained to recognise and report incidents.

4.7. Retaining records



Section 14 – Retention and restrictions of records

It is your responsibility to put processes in place regarding how long and in which format records of collected personal information should be kept.



What is a record?

A record is information created, received, and maintained by an organisation as evidence of actions or decisions to meet legal, regulatory, fiscal, operational, and historical requirements.

You must communicate to researchers that when identifiable personal information is no longer needed or subject to a retention period it must be destroyed or de-identified as soon as possible. It must not be possible to reconstruct the records in an intelligible form. You must ensure that once a record is only retained for proof or auditing, access to the record is restricted to people who need that personal information to perform their duties. However, there may be circumstances when it is necessary to retain records that contain identifiable personal information. Whenever practical, this personal information must be pseudonymised.



NB: Research-related records can be retained indefinitely if they are only retained for research purposes. You must put approval processes in place for using personal information again.

It is your responsibility to create a research records retention schedule that determines default rules for these categories of records:

- ✓ when the record is created (for example, when the research is concluded, when POPIA consent is obtained, when the research document is approved);
- ✓ how long the record should be retained (for example, indefinitely, at the conclusion of the research + 10 years); and
- ✓ why the record must be retained (for example, for proof, to comply with the general ethical guidelines for health researchers).

Researchers must record any deviation from these default rules in their research documents.

If personal information is held in the cloud or by a service provider, it is your responsibility to communicate to the researcher that they must securely delete it along with any backups. If personal information has been shared with collaborators during the research, they must also delete the personal information unless they have a legal justification to retain it and for the subsequent re-use of the personal information.

5. GLOSSARY

Biometrics	<p>Biometrics is the technique of identifying a person based on physical, physiological, or behavioural characteristics, including blood typing, fingerprinting, DNA/RNA analysis, retinal scanning, and voice recognition.¹⁷</p> <p>Biometric information is the information that results from specific technical processing relating to the physical, physiological, or behavioural characteristics of a research participant, such as facial images or dactyloscopic and genetic data when it is linked with other personal information to identify a data subject.</p>
Child or children	<p>A person(s) under the age of 18 who is not legally competent.¹⁸ If the person is under the age of 18 but emancipated, or if the Children's Act 38 of 2005 (or other legislation) gives the child the power to make certain decisions on their own behalf, they are not considered children for purposes of POPIA.</p>
De-identify	<p>in relation to personal information of a data subject, means to delete any information that—</p> <ul style="list-style-type: none"> (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, <p>and "de-identified" has a corresponding meaning;</p>
Genetic information	<p>Genetic information is derived from an individual's genetic material that can reveal health-related information, which is classified as special personal information</p>

¹⁷ Section 1.

¹⁸ Section 1.

Operator	An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. ¹⁹
PAIA	The Promotion of Access to Information Act 2 of 2000 and its regulations.
Personal information	<p>Personal information includes any information that relates to an identifiable, living individual or an identifiable, existing juristic person (e.g., a company or other type of organisation).²⁰</p> <p>POPIA provides the following examples:</p> <ul style="list-style-type: none"> • information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person • information relating to the education or the medical, financial, criminal or employment history of the person • any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or another particular assignment to the person • the personal opinions, views, or preferences of the person • 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 • the views or opinions of another individual about the person • the name of the person if it appears with other personal

¹⁹ Section 1.

²⁰ Section 1.

	information relating to the person or if the disclosure of the name itself would reveal information about the person
Plain language	A POPIA consent or notification will be in plain language if it is reasonable to conclude that an ordinary research participant of the group of research participants for whom the POPIA consent or notification is intended, with average literacy skills and minimal experience as a research participant, could be expected to understand the content and significance of the POPIA consent or notification, without too much effort. ²¹
POPIA	The Protection of Personal Information Act 4 of 2013 and its regulations.
POPIA consent	Consent required by POPIA.
Process or processing	Processing includes all activities that involve identifiable personal information – from collection to destruction. This includes to collect, receive, record, organise, collate, store, update, modify, retrieve, alter, consult, use, disseminate (transmit, distribute, or make available), merge, link, restrict, degrade, erase, or destroy the information. ²²
Pseudonymised or pseudonymisation	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.
Public body	Public body includes: ²³ <ul style="list-style-type: none"> any department of state or administration in the

²¹ This definition has been adapted from section 22 of the Consumer Protection Act 68 of 2008.

²² Section 1.

²³ Section 1.

	<p>national or provincial sphere of government</p> <ul style="list-style-type: none"> • any municipality in the local sphere of government • any other function or institution that is exercising a power or performing a duty in terms of the Constitution or a provincial institution • any other function or institution that is exercising a public power or performing a public function in terms of any legislation
Research	<p>Research includes the activities that are aimed at improving knowledge of any discipline through enquiry or systematic investigation. This framework applies regardless of whether the research is conducted by private or public bodies, whether the research is in the public interest or not, or whether the research is published or not.</p> <p>Research examples that the framework WILL apply to:</p> <ul style="list-style-type: none"> • All academic research conducted as part of any academic programme in any subject, including Agricultural Sciences, Earth Sciences, Economic Sciences, Education, Health/Medical Sciences, Humanities, Life Sciences, Mathematical Sciences, Physical Sciences, Social Sciences, Theology and Technological and Engineering Sciences. • Scientific research conducted by public or private bodies (regardless of whether the research is privately or publicly funded). • Commercial or industrial research aimed at developing or improving products or services. • Technological development and demonstration (e.g., prototype development, testing, user trials). <p>Research examples that the framework will NOT apply to:</p> <ul style="list-style-type: none"> • Profiling individuals to decide whether to market or offer

	<p>to supply a product or service to that specific individual.²⁴</p> <ul style="list-style-type: none"> • Statistical analysis.²⁵
Research consent	Consent as required in section 12(2)(c) of the Constitution or 'informed consent' as discussed in the Department of Health's, Health Research: Principles, Processes and Structures 2nd Edition (2015).
Research participant	<p>A data subject whose personal information is used for research. Where research involves animals, their owners or custodians will be considered research participants for purposes of this framework.</p> <p>'Data subject' is defined in POPIA as 'the person to whom personal information relates'. 'Person' is defined as either a natural person (individual) or juristic person (an organisation).</p>
Responsible party (Controller)	The responsible party is the private or public body or any person which 'alone or in conjunction with others, determines the purpose of and means for <u>processing</u> personal information'. ²⁶ The responsible party is the private or public body(s) or any person(s) who determines why and how personal information is processed. ²⁷
Research documentation	Research documentation or document is documentation that outlines the plan of a research study (can also be called research protocol, data management plans or similar documents).

²⁴ This activity is excluded from the framework because profiling in the context of generating 'leads' to market goods or services is not aimed at extending knowledge in general, but to extend knowledge about an individual. It should be covered in a Code of Conduct for marketing activities.

²⁵ Statistical analysis that is done on anonymous or aggregated information is not subject to the framework, because it does not involve identifiable personal information.

²⁶ Section 1 of POPIA.

²⁷ Section 1 of POPIA.

Special personal information

Special personal information is defined in section 1 of POPIA. It is an important definition because different legal justifications are available when a responsible party processes special personal information.

The following list contains examples of what special personal information of research participants typically is:

- Religious and philosophical beliefs: E.g., church membership, climate change denialism or ethical veganism.
- Race or ethnic origin: E.g., membership to a population group, culture, ancestry, territorial possession, language, or forms of dress.
- Trade union membership.
- Political persuasion: E.g., membership to a political party, political opinions or voting records.
- Health: E.g., any information on physical or mental injury, disease, disability or disease risk, including medical history, medical opinions, diagnosis and clinical treatment; medical examination data, test results, data from medical devices, or data from fitness trackers; information collected from a research participant when they register for health services or access treatment; any appointment details, reminders and invoices which reveal the health status of a research participant; any other information or behaviour that reveals a past, present or future physical or mental health status; administrative documents that reveal health status such as medical certificates, forms concerning sick leave or the reimbursement of medical expenses; inherited characteristics or genetic data.
- Sex life: E.g., information about a research participant's sexual activity, relationships, sexual orientation, or sexual proclivities.

	<ul style="list-style-type: none"> • <u>Biometric</u> information: The information that results from specific technical processing relating to the physical, physiological, or behavioural characteristics of a research participant, such as facial images or dactyloscopic or genetic data when it is linked with other personal information to identify a data subject. • Criminal behaviour of a data subject relating to the alleged commission of an offence or proceedings relating to an alleged offence. (Criminal convictions are not special personal information.)
Third parties	Third parties are people or organisations that have not previously had access to the personal information (including external collaborators, funders, service or system providers, and cloud hosting services).