



POPIA CODE OF CONDUCT FOR RESEARCH

A. ABOUT ASSAf

- A.1. The Academy of Science of South Africa ('ASSAf') is South Africa's official science academy. It is mandated under the Academy of Science of South Africa Act 67 of 2001 as amended by the Science and Technology Laws Amendment Act 16 of 2011.
- A.2. ASSAf currently has over 600 members from across all academic disciplines, including Agricultural Sciences, Earth Sciences, Economic Sciences, Education, Health/Medical Sciences, Humanities, Life Sciences, Mathematical Sciences, Physical Sciences, Social Sciences and Technological and Engineering Sciences.
- A.3. The objectives of the Academy are (amongst others) to promote common ground in scientific thinking across all disciplines, to promote the optimum development of the intellectual capacity of all people and to provide effective advice and facilitate appropriate action in relation to the collective needs, opportunities and challenges of all South Africans.¹ ASSAf views the balancing of the right to privacy of [Research Participants](#) against the collective public interest in scientific research as an integral part of these objectives.
- A.4. ASSAf believes that to protect the privacy of all Research Participants, this Code must apply to all Responsible Parties, who [Process Personal Information](#) for research purposes regardless of whether they are ASSAf members or not. To comply with Chapter 7 of the Protection of Personal Information Act 4 of 2013 ('[POPIA](#)') ASSAf has led a consultative process in the 'research sector' of South Africa to develop this Code of Conduct.



B. ABOUT THE POPIA CODE OF CONDUCT FOR RESEARCH

B.1. The purpose of the Code

B.1.1. The purpose of the Code is to:

- B.1.1.1. help [Research Institutions](#) and [Independent Researchers](#) comply with [POPIA](#);
- B.1.1.2. create legal certainty by ensuring that Research Institutions, Independent Researchers, and the Information Regulator have a consistent interpretation of POPIA and its impact on Research;
- B.1.1.3. foster collaboration;
- B.1.1.4. ensure that South Africa has adequate safeguards in place to protect research data; and
- B.1.1.5. ensure that Research Institutions and Independent Researchers are held accountable for non-compliance with POPIA.

B.2. Research must also comply with other legal and ethical obligations

- B.2.1. Research Institutions and researchers must comply with this Code *and* with other legislative and ethical obligations. For example, health Research must also comply with the National Health Act 61 of 2003.
- B.2.2. If this Code conflicts with another law, researchers must comply with the requirement that best protects the [Personal Information](#) of [Research Participants](#).²

B.3. The Code is binding

- B.3.1. Once the Information Regulator has issued a Code of Conduct, it has the force of law. Failing to comply with such a Code of Conduct is a breach of POPIA.³



B.3.2. While the Code refers to useful resources, they are not binding but are included as guidelines. Always refer to the latest version of a resource, even if the resource has been updated after this Code has been published. Most of the resources are from other jurisdictions and should be treated with care as the data protection regulations in those jurisdictions might differ from POPIA.

B.3.3. This Code will come into effect on **[insert date once agreed with the Information Regulator]**.

B.4. Defined terms and footnotes

B.4.1. If a word is Capitalised, it is defined in the [Glossary](#).

B.4.2. Endnotes have been included to document the rationale behind certain provisions and to facilitate the public and Information Regulator's review of the Code. Once the Information Regulator issues the Code, these endnotes will be removed.

TABLE OF CONTENTS

POPIA CODE OF CONDUCT FOR RESEARCH.....	1
A. ABOUT ASSAf.....	1
B. ABOUT THE POPIA CODE OF CONDUCT FOR RESEARCH.....	2
1. WHEN THE CODE APPLIES	5
2. DETERMINE WHO MUST ENSURE THAT RESEARCH COMPLIES WITH THE CODE .	6
3. DOCUMENT THE PURPOSE OF THE RESEARCH.....	12
4. PERFORM A PERSONAL INFORMATION IMPACT ASSESSMENT.....	13
5. ENFORCEMENT OF THE CODE	48
6. ADMINISTRATION OF THE CODE	55
7. GLOSSARY.....	57
Annexure A: When personal information is identifiable	64
Annexure B: Screening assessment.....	67
Annexure C: Minimality assessment	68
Annexure D: Records retention	70

1. WHEN THE CODE APPLIES

1.1. The scope of the Code

1.1.1. This Code applies to the [Processing](#) of [Personal Information](#) of identifiable [Research Participants](#) (individuals or organisations) for [Research](#) in South Africa. Processing includes collecting, creating, using, sharing, transforming, storing, or preserving Research Participants' personal information.

1.1.2. If the answer to all of the following questions are 'Yes', the Code applies:

1.1.2.1. [Is there processing?](#)

1.1.2.1.1. Processing includes collecting, creating, using, sharing, transforming, storing, or preserving Research Participants' identifiable Personal Information. The Code will apply to any Research where Personal Information is Processed after the effective date of the Code, regardless of when the Research started.

1.1.2.2. [Is there processing of identifiable personal information?](#)

1.1.2.2.1. Personal Information is any information related to an identifiable, living individual or an identifiable, existing juristic person (e.g., a company or other organisation). [POPIA](#) does not apply if [Personal Information](#) has been permanently de-identified. The Code acknowledges that to completely de-identify or anonymise Personal Information is difficult, if not impossible, considering technological advancements and the fact that increasing volumes of Personal Information are in the public domain. Researchers are therefore encouraged to assume that re-identification is possible and to still comply with the Code, rather than assume that the Personal Information has been de-identified. See Annexure A: When personal information is identifiable on how to determine whether Personal Information is identifiable.

1.1.2.3. [Is the purpose of processing personal information for research?](#)

1.1.2.3.1. [Research](#) includes the range of activities that a private or [Public Body](#)

conduct to extend knowledge through disciplined enquiry or systematic investigation.⁴

1.1.2.4. Is the processing taking place in South Africa?

1.1.2.4.1. The Code applies to [Research Institutions](#) or [Independent Researchers](#) based (domiciled) in South Africa.⁵ The Code also applies to foreign Research Institutions or Independent Researchers if they:

1.1.2.4.1.1. use automated or non-automated means in South Africa to Process Personal Information for Research. 'Means' refers to physical infrastructure, information technology infrastructure or human resources located in South Africa. The Code does not apply if the infrastructure is only used to forward Personal Information through South Africa;

1.1.2.4.1.2. use equipment or technology in South Africa to Process Personal Information; or;

1.1.2.4.1.3. collaborate with a South African Research Institution or Independent Researcher to Process the Personal Information in South Africa.⁶

1.1.3. See Annexure B: Screening assessment which can be used to screen whether Research is subject to the Code.

2. DETERMINE WHO MUST ENSURE THAT RESEARCH COMPLIES WITH THE CODE

2.1. This section covers:

2.1.1. what a [Responsible Party](#) is;

2.1.2. how to identify the Responsible Party in a [Research](#) project where there is collaboration; and

2.1.3. what the Responsible Party's obligations are.

2.2. The responsible party

2.2.1. [POPIA](#) introduces the legal concept of a Responsible Party. The Information

Regulator will hold the Responsible Party liable for non-compliance with the Code.⁷ The Responsible Party must ensure that [Research](#) complies with the Code before the Research begins and until it is completed.⁸ A Responsible Party can assign POPIA-related responsibilities to specific individuals (e.g., researchers) and hold them accountable if they fail to perform those responsibilities. However, those individuals are not accountable to the Information Regulator; they are accountable to the Research Institution.

- 2.2.2. The Responsible Party is the private or [Public Body](#)(s) or any person(s) who determines why and how [Personal Information](#) is [Processed](#).⁹ In most instances, the private or Public Body that employs, or directly controls the researchers will be the Responsible Party. The researchers will only be Responsible Parties in their individual capacity if a Responsible Party (private or Public Body) does not employ or control them; in other words if they are [Independent Researchers](#). The definition of 'employee' is in the Labour Relations Act 66 of 1995 or the Basic Conditions of Employment Act 75 of 1997. Even if a researcher is not an employee, they may be still under the control of a Research Institution. For instance, if they are bound by the policies and procedures of the Research Institution. This should be clearly stipulated in a contract with the researcher.
- 2.2.3. All Responsible Parties must perform the following tasks at an institutional level:
- 2.2.3.1. **Appoint an Information Officer and a Deputy Information Officer** (where the size of the Responsible Party justifies it) who must ensure compliance with the Code. The Information Officer or Deputy Information Officer's role description must be in writing and must explicitly refer to the Code. Foreign responsible parties 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.
- 2.2.3.2. **Create a POPIA compliance framework.** This framework must document how the Code will be implemented in the Responsible Party's policies, procedures, standards, templates, and other binding documents. These

documents must set out the responsibilities of different research-related roles, including research management (e.g., directors responsible for research activities), research ethics committees and other approval bodies, lead researchers (e.g., 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 the Responsible Party's compliance.

- 2.2.3.3. Have a **Promotion of Access to Information (PAIA) manual** that contains a general description of:
 - 2.2.3.3.1. **The type of [Research](#) conducted by the Responsible Party:** The PAIA manual must contain general information about the Responsible Party's research activities. It is not necessary to list all research activities.
 - 2.2.3.3.2. **Different types of [Research Participants](#):** E.g., the public, employees, clients, or students.
 - 2.2.3.3.3. **The different categories of Personal Information used in Research:** E.g., health information, financial information, political views, and contact details. List any [Special Personal Information](#).
 - 2.2.3.3.4. **Categories of [Third Parties](#) with whom Personal Information will be shared:** E.g., information technology service providers, open-access platforms and collaborators.
 - 2.2.3.3.5. **Planned [transborder information flows](#):** Some Third Parties may be in other countries. Responsible Parties should list all significant planned transborder information flows.
 - 2.2.3.3.6. **The security measures implemented to protect the Personal Information:** Responsible Parties should indicate that they comply with the Code and include a link to it.
 - 2.2.3.3.7. **How to exercise POPIA rights:** The PAIA manual must contain a detailed description of the procedure that Research Participants must follow to exercise their [POPIA rights](#).

- 2.2.3.4. See the Information Regulator's [PAIA manual templates for guidance on PAIA manuals](#).
- 2.2.3.5. Include a documented [research PIIA](#) (Personal information impact assessment) in its processes. Responsible Parties may decide who is responsible for ensuring that a research PIIA is performed, but the assessment must be done before the Research starts.
- 2.2.3.6. Ensure that everybody involved in research-related activities receives training on their data protection responsibilities.
- 2.2.3.7. Assess compliance with the Code and binding documents in [high-risk Research](#) regularly.

2.3. Identifying the responsible party when there is collaboration

- 2.3.1. It is possible to have multiple Responsible Parties (co-responsible parties). If they make joint decisions, there may be joint accountability to the Information Regulator.
- 2.3.2. In other instances, a Responsible Party may ask another private or Public Body or individual to Process Personal Information on their instruction; they are referred to as operators. An operator is not directly accountable to the Information Regulator, because they do not have a hand in why and how Personal Information is Processed. The Responsible Party who instructed them will be accountable.
- 2.3.3. Where there are multiple [Research Institutions](#) or Independent Researchers involved in the research activity, it could become complex to identify who is accountable. Here is a summary of the different roles and their legal implications:

Table 1: Identify the responsible party when there is collaboration

The role	The legal implications
Independent Responsible	Independent Responsible Parties share Personal

The role	The legal implications
Parties (Controllers) ¹⁰	<p>Information, but they do not make joint decisions about why and how Personal Information is Processed. They act independently, and each is accountable for compliance with the Code.</p>
Co-responsible Parties (or joint Controller)	<p>Co-Responsible Parties work towards a common purpose and make joint decisions when Processing Personal Information.¹¹ An example of this is where both parties decide the research question and how to conduct the Research.</p> <p>Co-Responsible Parties are jointly responsible for Processing Personal Information, and therefore ASSAf, the Information Regulator, and Research Participants can choose who to hold liable for non-compliance with the Code. They can also choose to hold co-Responsible Parties liable together.¹²</p> <p>Co-responsible Parties should conclude an agreement that sets out clearly who is responsible for compliance with which parts of the Code.</p>
Responsible Party and operator (or processor)	<p>An operator is 'a person or organisation that Processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party'. So, employees (as defined in labour law) are not operators.</p> <p>ASSAf, the Information Regulator and Research Participants will hold the Responsible Party liable if an operator does not comply with the Code.</p>

The role	The legal implications
	<p>The Responsible Party can hold the operator liable in a contract.</p> <p>If a Responsible Party (or Parties) uses an operator, they must agree in writing that the operator will comply with the Code's security safeguards section.</p>

2.3.4. If more than one Research Institution or Independent Researcher is conducting Research together, they must:

- 2.3.4.1. conduct an accountability assessment to identify the Responsible Party(s), co-Responsible Parties, and operators;
- 2.3.4.2. conclude agreements, and agree to policies or other binding obligations with co-Responsible Parties that identify who must comply with which sections of the Code;
- 2.3.4.3. conclude agreements, agree to policies or other binding obligations with all operators in which the operator agrees:
 - 2.3.4.3.1. to limit its use of the Personal Information to instances where the Responsible Party gave written authorisation;
 - 2.3.4.3.2. that the Personal Information is confidential and must not be shared with [Third Parties](#) without the Responsible Party's written authorisation;
 - 2.3.4.3.3. to comply with the [security safeguards section](#) of the Code;
 - 2.3.4.3.4. to notify the Responsible Party immediately in the case of a [security compromise](#);
 - 2.3.4.3.5. to take any additional steps the Responsible party requires to comply with the Code;
- 2.3.4.4. comply with the section of the Code on [transborder information flows](#) where Personal Information is transferred to a [Third Party](#) located in

another country.

3. DOCUMENT THE PURPOSE OF THE RESEARCH

3.1. If the Code applies to [Research](#), the [Responsible Party](#) must ensure that researchers document the following information in [Research Protocols](#):

Table 2: Document the purpose of the research

What must be documented	Some guidance
What Personal Information is being collected.	Provide researchers with a checklist based on the definition of Personal Information to encourage them to provide enough detail to comply with the rest of the Code.
The purpose, aim, or objective for collecting the Personal Information. ¹³	The purpose, aim or objective must be specific and explicitly defined. ¹⁴ It must be possible for someone who is not involved in the Research (e.g., the Information Officer, a Deputy Information Officer, or the Information Regulator) to gauge what Personal Information is necessary to achieve this purpose.
The nature, extent, and context of the Processing of Personal Information?	Researchers should include the following: <ul style="list-style-type: none">• the number of Research Participants and how they will be recruited and contacted;• how they will collect, use and store Personal Information;• the nature and the source of the Personal Information;• if they share the Personal Information, with whom do they share it (including external collaborators, funders, service or system

What must be documented	Some guidance
	<p>providers, and cloud hosting services);</p> <ul style="list-style-type: none"> • note any concerns relating to the security of the Personal Information; • mention whether any new or innovative technology will be used to Process the Personal Information.

4. PERFORM A PERSONAL INFORMATION IMPACT ASSESSMENT

- 4.1. All [Research](#) must go through a [Personal Information](#) impact assessment ('research PIIA') to ensure Responsible Parties manage the risk to [Research Participants](#) appropriately by including appropriate safeguards in Research Protocols.¹⁵
- 4.1.1. The [Responsible Party](#) must ensure that a research PIIA is performed for every research activity (e.g., a project or study).
- 4.1.2. To ensure that the Code does not stifle Research, a risk-based approach is essential. Therefore, the prescribed research PIIA should follow the approach taken in the European Union, where only high-risk Research requires a complete gap analysis by an Information Officer or Deputy Information Officer of the Responsible Party or a senior employee(s) formally designated to perform this task on their behalf.¹⁶ The Code prescribes a three-phase research PIIA:
- 4.1.2.1. Phase 1: Preliminary risk assessment to determine whether the Research should be classified as high-risk.
- 4.1.2.2. Phase 2: Gap analysis to determine whether the Research Protocol complies with [POPIA](#).
- 4.1.2.3. Phase 3: Implementation and monitoring to record safeguards and a monitoring plan in the Research Protocol.

4.2. Preliminary risk assessment

- 4.2.1. The preliminary risk assessment aims to identify high-risk [Research](#) and encourage researchers to re-evaluate whether their Research warrants high-risk practices.
- 4.2.2. If a research activity is high-risk, an Information Officer or Deputy Information Officer of the Responsible Party or a senior employee(s) formally designated to perform this task on their behalf must:
- 4.2.2.1. perform a [gap analysis](#) and sign off on the [Research Protocol](#);
 - 4.2.2.2. monitor annually whether the researchers have implemented the Research Protocol;
 - 4.2.2.3. ensure that the Personal Information is [Pseudonymised](#) unless there is a compelling reason why it is not feasible or appropriate; and
 - 4.2.2.4. ensure that the Personal Information will be encrypted unless there is a compelling reason why it is not feasible or appropriate.
- 4.2.3. The preliminary risk assessment must include the following questions¹⁷
Research that scores more than five 'Yes' answers will be considered high-risk.

Table 3: Preliminary risk assessment

#	The questions	Some guidance	Yes	No
1	Will the Research Participants include Children or other vulnerable groups?	Other vulnerable groups may include the elderly, illiterate individuals, pregnant women, disabled or mentally disabled individuals or individuals with mental illness that impedes their capacity and individuals in poor health or belonging to economically and educationally disadvantaged groups.		

#	The questions	Some guidance	Yes	No
2	<p>Will the Research involve Processing Special Personal Information or information of Children on a large scale?</p>	<p>Provide researchers with a checklist of Special Personal Information.</p> <p>Processing is considered on a large scale if:</p> <ul style="list-style-type: none"> • many Research Participants are involved; or • a large proportion of a population is involved; or • 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 (e.g., longer than the average research activity). 		
3	<p>Will the Research involve the evaluation or scoring of Personal Information to make automated decisions with legal consequences or that will have a significant effect on Research Participants?</p>	<p>This includes Research that uses profiling and predictive analysis (e.g., cardiovascular disease risk calculators) 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.</p> <p>For the answer to be 'Yes', the automated decision must affect the research participant's circumstances, behaviour, or choices. It might affect their financial</p>		

#	The questions	Some guidance	Yes	No
		<p>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'.</p> <p>Note that profiling and predictive analysis for marketing purposes are excluded from the Code's scope.</p>		
4	Will the Research involve Processing where researchers are not getting Research Participants' Personal Information directly from them?	Typically when Research Participants' Personal Information is collected from another source (i.e., the internet, social media platforms, the Research Participants' employer or organisations that render services to the research participant).		
5	Will the Personal Information of Research Participants be disclosed to Third Parties ?	Personal Information is transmitted to another organisation or person (Third Parties), or they are given access to the Personal Information.		
6	Are any people or organisations that will have access to the Personal Information located in another country?	Personal Information is transmitted to another country or an organisation or person in another country is allowed to access the Personal Information.		
7	Will unique identifiers be used to link, combine, compare, or match Personal Information from	Different sets of Personal Information held by other organisations or persons are linked by using unique identifiers to form a new dataset.		

#	The questions	Some guidance	Yes	No
	multiple sources?	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.		
8	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.		
9	Would the Processing of Personal Information contemplated by the researchers be outside of the reasonable expectations of the individuals?	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?		
10	Will the Research involve contacting or interacting with individuals in ways they might find intrusive?	For instance, where Personal Information is collected by systematically monitoring the Research Participants in publicly accessible places without their knowledge.		

4.2.3.1. Regardless of the outcome, Responsible Parties must keep a reliable record of the preliminary risk assessment.

4.3. Perform a gap analysis

4.3.1. The purpose of a gap analysis is to measure the current or envisioned research activities against certain conditions to determine where there is room for improvement. These conditions are accountability, processing limitation, purpose specification, further processing limitation, information quality, openness and notification, security safeguards and research participant participation.

4.3.2. Condition 1: Accountability

4.3.2.1. Where Personal Information will be shared, the Information Officer or Deputy Information Officer must perform an [accountability assessment](#) to identify the Responsible Party(s).

4.3.2.2. When the Personal Information of Research Participants is not shared with [Third Parties](#), accountability will lie with the Research Institution or Independent Researcher.

4.3.3. Condition 2: Processing limitation

4.3.3.1. Lawfulness of processing

4.3.3.1.1. Responsible parties must ensure that the research PIIA is embedded in its policies and procedures and must monitor whether research PIIAs are performed correctly.¹⁸

4.3.3.2. Minimal processing (minimality)

4.3.3.2.1. Personal Information may only be used in Research if, given the purpose of the Research, the Personal Information is adequate, relevant, and not excessive.¹⁹ Responsible Parties must ensure that the Processing of identifiable Personal Information is necessary and proportional.

4.3.3.2.2. For further guidance, see Annexure C: Minimality assessment attached to the Code.²⁰

4.3.3.3. [POPIA Consent](#), justification, and objection

- 4.3.3.3.1. Responsible parties must ensure that researchers rely on the correct legal justification for Processing Personal Information. The legal justifications that are available depend on whether the research activity includes [Special Personal Information](#).
- 4.3.3.3.2. This section of the Code only applies where the Personal Information of Research Participants was originally collected for research purposes and is being used for the first time. If Personal Information collected for another purpose is reused, the Responsible Party must perform a [further Processing assessment](#).
- 4.3.3.3.3. **Important:** 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).²¹ Research must comply with this Code *and* with any other legislative and ethical obligations that may apply.
- 4.3.3.3.4. If none of the legal justifications apply, it is illegal for the Research to continue.
- 4.3.3.3.5. Any of the following legal justifications must apply when the Research does NOT include Special Personal Information:²²

Table 4: Legal justification that must apply when the Research does NOT include Special Personal Information

The legal justification	Some guidance
Research Participants will be asked for POPIA Consent. ²³	<p>The researcher should ask the research participant for POPIA Consent to use their Personal Information where possible. However, it is not an absolute requirement in terms of POPIA.²⁴</p> <p>To comply with POPIA, the POPIA Consent must be: ²⁵</p> <p>Voluntary: Research Participants should not be</p>

The legal justification	Some guidance
	<p>coerced into providing POPIA Consent.</p> <p>Responsible Parties should take extreme care when offering incentives to ensure that they do not undermine the free will of the Research Participants, or exploit their vulnerability.</p> <p>Research Participants must be able to withdraw their POPIA Consent without too much effort, after which the Responsible Party must stop Processing their Personal Information.</p> <p>Specific: The POPIA Consent must clearly set out the specific purpose for which the Personal Information is Processed. POPIA Consent for future use is allowed as long as the future uses of the Personal Information are not speculative, are described as fully as possible, and further use of the Personal Information is restricted. (Also, see the section of the Code on further Processing and when it is allowed.)</p> <p>Informed: Research Participants should be told who the Responsible Parties are that will rely on the POPIA Consent, the purpose(s) for which POPIA Consent is asked, the type of Personal Information that 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.</p> <p>Explicit: The POPIA Consent must be given</p>

The legal justification	Some guidance
	<p>through a clear, unambiguous, affirmative act. It cannot be provided by default, and silence or inactivity cannot be taken as POPIA Consent. It should be in writing or another recorded format. Responsible Parties must maintain a record of POPIA Consent obtained from Research Participants during the research and for as long as identifiable Personal Information relating to that research participant is retained.</p> <p>For further guidance on POPIA Consent, see:</p> <ul style="list-style-type: none"> • European Data Protection Supervisor A Preliminary Opinion on data protection and scientific research (from page 9) • European Data Protection Board Guidelines on Consent
<p>The Research is required by law.²⁶</p>	<p>If the Responsible Party is explicitly required to conduct Research in terms of the Constitution, common law, customary law, legislation, or a court decision, POPIA Consent is not required. However, the Research must be <i>necessary</i> to comply with the obligation. In other words, if the law does not require that identifiable Personal Information must be Processed, a Responsible Party cannot rely on this justification.</p> <p>If a Responsible Party wants to rely on this justification, they must ensure that:</p> <ul style="list-style-type: none"> • they identify the specific legal provision on

The legal justification	Some guidance
	<p>which they are relying;</p> <ul style="list-style-type: none"> • the Processing is necessary to comply with the legal obligation; • there is no less invasive way to comply with the legal obligation; and • they document the decision to rely on this justification. <p>This is a robust justification. The Research Participant does not need to provide POPIA Consent and will not have a right to object to the Research.</p>
<p>The Research is conducted by a Public Body performing a public law duty.²⁷</p>	<p>If the Responsible Party is a Public Body performing a public law duty, the Responsible Party does not have to obtain a POPIA Consent. However, Research Participants will have a right to object to the Research based on their situation.²⁸ When a Research Participant objects, the Responsible Party must stop Processing their Personal Information.</p>
<p>The Research is in the legitimate interest of the Responsible Party, of a Third Party to whom the Personal Information is supplied, or of the Research Participants.²⁹</p>	<p>If the Responsible Party or a Third Party stands to benefit from the Research, they can rely on this legitimate interest to justify the Processing if the limitation on the privacy of the Research Participants is reasonable.³⁰</p> <p>While a POPIA Consent is not required, Research Participants will have a right to object to the Research based on their situation.³¹ When a</p>

The legal justification	Some guidance
	<p>Research Participant objects, the Responsible Party must stop Processing their Personal Information.</p> <p>When a Responsible Party relies on this justification, they must perform a legitimate interest assessment.</p> <p>³² A legitimate interest assessment has three steps:</p> <ul style="list-style-type: none"> • Identify the legitimate interest: What are the benefits to the Responsible Party, Third Party or data subject? Are there any wider public benefits? How significant are these benefits? What would the impact be 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 the legitimate interests of the Responsible Party or a Third Party? Is there another less intrusive way to achieve the same results? • Apply a balancing test: Does the impact on Research Participants override the interests of the Responsible Party or a Third Party? Is any of the Personal Information particularly sensitive or private? Are the Research Participants Children or vulnerable in any other way? 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

The legal justification	Some guidance
	<p>impact on the Research Participant? Can the Responsible Party adopt safeguards to minimise the impact?</p> <p>See the Information Commissioner's Office How do we apply legitimate interest in practice for guidance.</p>

4.3.3.3.6. One of the following legal justifications must apply when the Research includes [Special Personal Information](#).³³

Table 5: The legal justifications that must apply when the Research includes Special Personal Information

The legal justification	Some guidance
Will Research Participants be asked for POPIA Consent? ³⁴	The same guidance as discussed in the table above will apply.
Is the Research in the public interest? ³⁵	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). ³⁶
Is it impossible, or would it require a disproportionate effort to get POPIA Consent? ³⁷	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. ³⁸

The legal justification	Some guidance
Has the Research Participant deliberately made the Personal Information public? ³⁹	<p>For this legal justification to apply, the following requirements must be met:</p> <ul style="list-style-type: none"> • The Personal Information must have been made public: There must be no impediment (e.g., a paywall or a data wall) to the accessibility of the Personal Information.⁴⁰ • By the data subject: If someone else published the Personal Information, this legal justification does not apply. The Responsible Party must be able to prove who published the Personal Information. • Deliberately: There must be evidence of an unmistakably deliberate and affirmative action by the data subject.
Does one of the legal justifications specific to Special Personal Information apply as outlined in sections 28 to 33 of POPIA?	If none of the legal justifications above apply, Responsible Parties should interrogate whether one of the other legal justifications that apply to Special Personal Information applies. ⁴¹

4.3.3.3.7. One of the following legal justifications must apply when the Research includes the Personal Information of a [Child](#).⁴² A Child is 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.⁴³

4.3.3.3.8. **Important:** Researchers are responsible for verifying the age of Research Participants to ensure that the correct legal justifications are applied. For instance, 'legitimate interest' cannot be used regarding

the Personal Information of a Child. Age verification should not lead to excessive Processing of Personal Information and must be proportionate to the nature of and risks involved in the Research.

Table 6: The legal justifications that must apply when the Research includes the Personal Information of a Child

The legal justification	Some guidance
Will the Research Participant's parent or guardian be asked for POPIA Consent? ⁴⁴	<p>If a researcher wants to rely on POPIA Consent to justify the Research, the POPIA Consent must be obtained from a 'competent person'.⁴⁵ In terms of POPIA, this will be a person with parental responsibilities in terms of the Children's Act 38 of 2005.</p> <p>The same guidance as discussed in the table above will apply.</p>
Is the Research in the public interest? ⁴⁶	<p>What constitutes as 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 (as opposed to a few or a single entity or person) and should be pursued in the spirit of equality and justice.⁴⁷</p>
Is it impossible, or would it require a disproportionate effort to get POPIA Consent? ⁴⁸	<p>POPIA Consent is not required if obtaining it is impossible or would require a disproportionate effort. Given the inherent vulnerability of Children, it must be virtually impossible, as opposed to merely impractical or costly, to obtain POPIA Consent before this legal justification applies.⁴⁹</p>
Has the Child made the	For this legal justification to apply, the following

The legal justification	Some guidance
Personal Information public deliberately with the POPIA Consent of a competent person? ⁵⁰	requirements must be met: <ul style="list-style-type: none"> • The Personal Information must have been made public: There must be no impediment (e.g., a paywall or a data wall) to the accessibility of the Personal Information.⁵¹ • By the Child: If someone else published the Personal Information, this legal justification does not apply. The Responsible Party must be able to prove who published the Personal Information. • Deliberately: There must be evidence of an unmistakably deliberate, affirmative action by the data subject. • With the POPIA Consent of a competent person: Someone with parental responsibility must have consented to the disclosure made by the Child.

4.3.3.4. The direct collection rule

4.3.3.4.1. A researcher may only collect a Research Participant's Personal Information from another source under certain circumstances.⁵² Collecting Personal Information from other sources is considered high risk because:

4.3.3.4.1.1. the Research Participants may not be aware that their Personal Information is being collected;

4.3.3.4.1.2. the other source may not be reliable (i.e., the Personal Information may not be complete or accurate).

4.3.3.4.2. Researchers must maintain a record of the sources of Personal Information used in the Research.

4.3.3.4.3. Personal Information may be collected under any of the following circumstances:⁵³

Table 7: The direct collection rule

The question	Some guidance
<p>Is the Personal Information available in or derived from a public record?⁵⁴</p>	<p>A public record is a record that:⁵⁵</p> <ul style="list-style-type: none"> • Is accessible in the public domain: If there is restricted access (e.g., 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. • Is in the possession of or under the control of a Public Body:⁵⁶ 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. <p>The internet or a social media platform is not a public record.</p>
<p>Did the Research Participant make the Personal Information public deliberately?⁵⁷</p>	<p>The Responsible Party will have to prove that the Research Participant made the Personal Information public themselves or consented that an intermediary can make the Personal Information public intentionally. This may be the case with Personal Information published on the</p>

The question	Some guidance
	internet, but this will not always be the case.
Did the Research Participant POPIA Consent to the collection of Personal Information from another source? ⁵⁸	<p>This POPIA Consent must meet the requirements discussed in the context of legal justifications.</p> <p>It will not be 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.</p>
Will the benefits of collecting Personal Information from another source outweigh the impact on the Research Participant's privacy? ⁵⁹	<p>Researchers should document the positive and negative impacts of collecting the Personal Information from another source. If the positive implications outweigh the negative repercussions, collecting the Personal Information from another source is justified.</p>
Is collecting the Personal Information from another source in the legitimate interest of the Responsible Party or of a Third Party to whom the information is supplied? ⁶⁰	<p>Legitimate interest assessments are discussed in the context of legal justifications. However, if the researcher relies on legitimate interests as a legal justification <i>and</i> a basis for collecting the Personal Information from another source, they must conduct two legitimate interest assessments.</p>
Would collecting the Personal Information directly from the Research Participant undermine the Research? ⁶¹	<p>In some instances, it may be detrimental to the Research if the Personal Information is (only) collected directly from the Research Participants. E.g., if there are strong reasons to believe that Research Participants will not be truthful or do not have access to reliable Personal Information (e.g., reliable location or behavioural information).</p> <p>Researchers must document why collecting the</p>

The question	Some guidance
	Personal Information directly from the Research Participant will undermine the Research.
Is it impossible to collect the Personal Information directly from the Research Participant? ⁶²	<p>Researchers can rely on this exception if it would be virtually impossible to obtain the Personal Information directly from the Research Participants, e.g., where researchers do not have the contact details of Research Participants and no way to get the contact details. The high cost of contacting Research Participants is insufficient to rely on this exception.</p> <p>In other instances, Research Participants may not have Personal Information about themselves (e.g., accurate location or behavioural information).</p>

4.3.4. Condition 3: Purpose specification

4.3.4.1. Document the purpose of the research

4.3.4.1.1. This is discussed in the section on [documenting the purpose of the Research](#).

4.3.4.2. Retention and restriction of records of research

4.3.4.2.1. Responsible Parties must document how research records will be retained once the Research has been concluded. The principles that Responsible Parties document must balance the [principle of minimal Processing and the](#) need for the Responsible Party to preserve an authoritative record of its research activities.⁶³

4.3.4.2.2. **Important:** 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. This section of the Code discusses how long records relating to Research must be kept after the Personal Information is no longer in active use. For

example, when Personal Information is no longer being analysed or shared with other researchers. When identifiable Personal Information is shared on 'open access' or other repositories for further use in subsequent Research, it is not an archive; that Personal Information is still in active use. [Further Processing of Personal Information](#) for Research is only allowed if it complies with the requirements set out in the next section.

4.3.4.2.3. 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 record in an intelligible form. Responsible Parties must use the same [test for identifiability](#) when determining whether Personal Information has been destroyed or de-identified. They must ensure that once a record is only retained for purposes of proof or auditing, access to the record is restricted to people who need that Personal Information to perform their duties.⁶⁴

4.3.4.2.4. However, the Code acknowledges that there may be circumstances when it is necessary to retain records that contain identifiable Personal Information. Whenever practical, this Personal Information must be [Pseudonymised](#).

4.3.4.2.5. **Important:** Research-related records can be retained indefinitely if they are only retained for research purposes. Responsible Parties must have approval processes for using Personal Information again.⁶⁵ [Further Processing of Personal Information](#) is discussed in the next section.

4.3.4.2.6. See Annexure D: Records retention for guidelines on the types of research-related records that should be retained.

4.3.5. Condition 4: Further Processing limitation (secondary use)

4.3.5.1. When the purpose for which Personal Information is used changes or the Personal Information is reused for another purpose, it is referred to as 'further Processing'.⁶⁶ Section 15(3)(e) provides that the reuse of

Personal Information for research purposes will be allowed if:

- 4.3.5.1.1. the Personal Information will only be used for research purposes; and
- 4.3.5.1.2. the Personal Information will not be published in an [identifiable](#) form.
- 4.3.5.2. **Important:** Even though reuse of the Personal Information is permitted without POPIA Consent from the Research Participant, the rest of POPIA still applies. For instance, the Research Participant may have to be notified of further Processing.
- 4.3.5.3. If researchers intend to use Personal Information that was collected from a previous research project or altogether different purpose, the researcher must provide the following information in the new Research Protocol:
 - 4.3.5.3.1. 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);
 - 4.3.5.3.2. how the researcher will ensure that the Personal Information will only be used for research purposes and that it will not be published in an identifiable form (e.g., contractual undertakings or that there will be a data access committee, or both);
 - 4.3.5.3.3. how the researcher will comply with the [notification requirement](#); and
 - 4.3.5.3.4. whether the researcher has permission from the Responsible Party who initially Processed the Personal Information.

4.3.6. Condition 5: Information quality

- 4.3.6.1. In addition to ensuring that the Personal Information collected for the Research is adequate, relevant, and not excessive, given the purpose of the Research, Responsible Parties must also take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary.⁶⁷ The degree of accuracy required depends on the purpose of the Research and the consequences for Research Participants and society if the Personal

Information is inaccurate.

4.3.6.2. See the information quality guideline for further information.

4.3.6.3. Responsible Parties must ensure that researchers include safeguards in their Research Protocols. Responsible Parties must ensure that researchers implement the following safeguards:⁶⁸

Table 8: Condition 5: Information quality

Safeguard	Some guidance
Use reliable sources	<p>If Personal Information is collected from sources other than the Research Participants, additional safeguards must be put in place to guarantee the reliability of the Personal Information. This could include:</p> <ul style="list-style-type: none">• 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. <p>Researchers must maintain a record of the source of all Personal Information.</p>
Data quality reviews	<p>Responsible Parties must make sure that researchers document data quality reviews in their Research Protocols to ensure that the Personal Information the researchers have collected is complete, accurate, not misleading and updated where necessary.</p> <p>How frequently data quality reviews must be</p>

Safeguard	Some guidance
	<p>performed will depend on the type of Personal Information that is collected and how quickly it will age, and the potential harm it could cause to Research Participants if the Personal Information is incorrect. E.g., ID numbers do not change, so regular data quality reviews are not necessary.</p> <p>Researchers must document in their Research Protocol that data quality reviews were considered and document the reasons for the approach they took.</p>
Provide Research Participants with access	<p>Research Participants have the right to access their own Personal Information.⁶⁹ Even though this right is not absolute, Research Participants should have effective access to their Personal Information by default and the ability to control the accuracy of their Personal Information and correct it if necessary. If effective access is impractical or would harm the Research Participant, the reasons for not granting access by default should be documented in the Research Protocol.</p>
Master data management	<p>The quality of Personal Information should be managed centrally. If copies are allowed, it must be for specific and documented reasons with strict version control.</p>
Design questions and answer formats for accuracy	<p>The questions that Research Participants must answer should be designed to increase accuracy. For instance, questions should not be</p>

Safeguard	Some guidance
	<p>ambiguous, and unless the research calls for another answer format, Research Participants should be presented with concise predetermined choices, instead of free text fields.</p>
<p>Techniques to minimise the risk of error or discriminatory effect (bias)</p>	<p>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, the following measures must be in place. Researchers must:⁷⁰</p> <ul style="list-style-type: none"> • understand the technology and algorithms; • provide Research Participants with sufficient information about the underlying logic of the automated decisions; • 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 representations about the outcome of the automated

Safeguard	Some guidance
	decision.

4.3.7. Condition 6: Openness and notification

4.3.7.1. Openness

4.3.7.1.1. Responsible Parties must ensure that:

- 4.3.7.1.1.1. Research Participants understand how Personal Information is Processed for Research by publishing general information in their [PAIA](#) manual;⁷¹
- 4.3.7.1.1.2. they can demonstrate compliance with this Code in their policies, procedures, templates, or similar governance documents (together, this forms the Responsible Party's POPIA Compliance Framework).⁷²

4.3.7.1.2. Both requirements are met by complying with the [accountability checklist for Responsible Parties](#).

4.3.7.2. Transparency (notification)

4.3.7.2.1. POPIA provides that the notification duty imposed in section 18(1) does not apply if the Personal Information will 'be used for historical, statistical or research purposes'.⁷³ However, providing information to Research Participants will often be essential to provide consent (whether to POPIA Consent or Research Consent). In other words, when researchers rely on POPIA Consent, they must ensure that Research Participants are provided with sufficient information to make an informed decision.

4.3.8. Condition 7: Security safeguards

4.3.8.1. Appropriate technical and organisational safeguards

4.3.8.1.1. POPIA provides that a [Responsible Party](#) must establish appropriate technical and organisational safeguards. When considering what 's

'appropriate', Responsible Parties may set different requirements depending on the outcome of the [preliminary risk assessment](#). Responsible Parties must also obtain expert advice on how to achieve the level of security that is proportionate to the risk to the Research Participant.

4.3.8.1.2. The following technical and organisational safeguards must be put in place by (or on behalf of) Responsible Parties:⁷⁴

Table 9: Condition 7: Security safeguards

Safeguards	Some guidance
<p>Ensure ongoing confidentiality, integrity, availability and resilience of processing systems and software</p>	<p>Responsible Parties must put the following safeguards in place:</p> <ul style="list-style-type: none"> <p>Access control procedures and access logging: Responsible Parties must have policies and procedures in place that regulate access to Personal Information used in Research. Responsible Parties must apply the principles of 'role-based access' (i.e., need to know) and 'least privilege' (e.g., limited ability to modify Personal Information) in this procedure. Responsible Parties must ensure that users (e.g., researchers) are identified before they are granted access to identifiable Personal Information. For access control a one-factor authentication (e.g., a strong password) is required, but a two-step authentication (i.e., two-factor authentication) is recommended. If the Responsible Parties did not implement a two-step authentication, they must document why it was not possible. Responsible Parties must</p>

Safeguards	Some guidance
	<p>document who has access to identifiable Personal Information and log any changes to the Personal Information.</p> <ul style="list-style-type: none"> • Third-party risk management: If Responsible Parties use operator(s) (e.g., a cloud service provider), the Responsible Parties must conclude an agreement in which the Third Party undertakes to comply with the security safeguards section of the Code. • Use of acceptable software: Responsible Parties must have rules in place about what software is acceptable to use in Research and must provide guidance to researchers on how to use that software securely. All software should be approved for use by the Responsible Parties. • Storage security: Responsible Parties must store Personal Information in a way that prevents unauthorised access (e.g., authentication and access control, use of passwords to access electronic files, local encrypted storage, and database encryption). Responsible Parties must ensure that these safeguards are applied to local PCs, portable storage devices and cloud-based computing services. • Security for transfers/communication: Responsible Parties must ensure safe electronic communication for transferring Personal Information (e.g., encrypted

Safeguards	Some guidance
	<p>communication, secure file transfer protocols, VPNs, firewall systems, anti-virus, and anti-malware systems) and that Personal Information is protected when it is physically transferred.</p> <ul style="list-style-type: none"> <p>Mobile devices, home or remote working and removable media: Responsible Parties must have policies and procedures in place to manage security risks associated with devices used by researchers. Protection must be in place to avoid unauthorised access (e.g., encryption and remote wiping capabilities). Security measures must be in place to protect Personal Information when researchers are working from home or working remotely (e.g., VPN and two-factor authentication). Personal Information may only be stored on removable media if absolutely necessary. Responsible Parties 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 the Responsible Parties to provide support and update devices remotely.</p> <p>Physical security: Responsible Parties must secure areas that contain high-risk Research by appropriate entry controls and sign-in procedures. Paper records containing Personal Information must be secure, and access must be controlled. A clean desk and</p>

Safeguards	Some guidance
	<p>clear screen policy should be in place where Personal Information is Processed.</p> <ul style="list-style-type: none"> • Back-ups: Responsible Parties must ensure that systems are resilient and backed up. Responsible Parties must be able to restore access and availability to Personal Information in a timely manner in the event of a physical or technical incident.
<p>Pseudonymisation and anonymisation</p>	<p>Pseudonymisation must be the default for all high-risk Research. Where high-risk Research deviates from Pseudonymisation, the reasons must be documented. Responsible Parties must encourage Pseudonymisation in all other Research.</p> <p>Research Protocols must state when the Personal Information will be anonymised (e.g., before publication). Personal Information must be anonymised as soon as possible. Responsible Parties must provide guidance on acceptable Pseudonymisation and anonymisation techniques.</p>
<p>Encryption</p>	<p>Encryption must be the default for all high-risk Research. Where Responsible Parties deviate from encryption, their reasons must be documented. Responsible Parties must encourage encryption in all other Research.</p>
<p>Restricted environment for high-risk Research</p>	<p>Responsible Parties that regularly engage in high-risk Research are strongly encouraged to establish restricted environments where Research can be stored and transferred. These restricted environments</p>

Safeguards	Some guidance
	<p>must be certified to the ISO27001 Information Security Management standard or other similar standards.</p> <p>It is likely that this will become a requirement in future revisions of the Code.</p>

4.3.8.2. Security compromises

4.3.8.2.1. This section applies to 'security compromises' where there are reasonable grounds to believe that the Personal Information of Research Participants has been accessed or acquired by an unauthorised person.⁷⁵

4.3.8.2.2. Responsible Parties must implement an incident reporting and response procedure.

4.3.8.2.3. The response procedure for a security compromise must include the following:

Table 10: Security compromises

Step	Some guidance
Establish an incident reporting procedure	Responsible Parties must specify where and how incidents must be reported.
Mitigate risks immediately	<p>Responsible Parties must take steps to:</p> <ul style="list-style-type: none"> • mobilise security compromise response teams; • notify law enforcement if there is criminal conduct; • restore the confidentiality, integrity and availability of the Personal Information

Step	Some guidance
	<p>or the information system;</p> <ul style="list-style-type: none"> • assess the scope of the compromise; and • preserve evidence.
Conduct a risk assessment	<p>Responsible Parties must conduct a risk assessment to assess the risk posed to Research Participants. This includes assessing:</p> <ul style="list-style-type: none"> • the identity of the unauthorised person(s) and their possible motives; • the possible consequences of the security compromise; and • a description of measures that the Responsible Parties or Research Participants can take to mitigate the consequences.
<p>Notify ASSAf, the Information Regulator and co-Responsible Parties of the suspected security compromise</p> <p>AND</p> <p>Notify Research Participants</p>	<p>Responsible Parties must, after completing the immediate risk mitigation and the risk assessment, send out the following notification as soon as reasonable after they discovered the compromise.</p> <p>The notification must include:</p> <ul style="list-style-type: none"> • the steps the Responsible Parties 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;

Step	Some guidance
	<p>and</p> <ul style="list-style-type: none"> • a communication plan and the wording of messages to Research Participants. <p>Responsible parties must send the breach notification to:</p> <ul style="list-style-type: none"> • The Information Regulator: POPIACompliance@inforegulator.org.za • ASSAf: [insert email address] <p>Unless a Public Body in law enforcement or the Information Regulator asks for a delay, responsible parties must notify Research Participants of the security compromise as soon as reasonably possible after the security compromise was discovered.</p> <p>The notification to Research Participants must comply with sections 22(4) and (5) of POPIA.</p>
Report to ASSAf and the Information Regulator on measures to prevent future security compromises and agree on a monitoring plan	ASSAf or the Information Regulator may require that the Responsible Parties provide a report on measures to prevent future security compromises and may require that the Responsible Parties provide progress reports to ASSAf or the Information Regulator.

4.3.8.2.4. Responsible parties must ensure that researchers and other staff are trained to recognise and report incidents.

4.3.9. Condition 8: Research participant participation (POPIA rights)

4.3.9.1. Researchers must ensure that Research Participants have the

opportunity to exercise their POPIA rights. The procedure that Research Participants must follow to do so should be effortless and free.

- 4.3.9.2. Responsible Parties who regularly engage in Research should create a centralised process that all Research Participants can use to exercise their rights. This process should be included in the Responsible Party's [PAIA manual](#). In the absence of a centralised process, the Responsible Party must implement a process for each research project.
- 4.3.9.3. Research Participants have the right to:
 - 4.3.9.3.1. withdraw their POPIA Consent;
 - 4.3.9.3.2. object to Processing based on reasonable grounds relating to their situation;
 - 4.3.9.3.3. access their own Personal Information (unless one of the grounds for refusing access in PAIA applies);
 - 4.3.9.3.4. correct or delete their Personal Information; and
 - 4.3.9.3.5. make representations about automated decisions with a legal or substantial effect.
- 4.3.9.4. [The right to withdraw POPIA Consent](#)
 - 4.3.9.4.1. Research Participants have the right to withdraw their POPIA Consent at any time,⁷⁶ in which case the Responsible Party must stop Processing the Research Participants' Personal Information.
- 4.3.9.5. [The right to object to processing based on reasonable grounds relating to their situation](#)
 - 4.3.9.5.1. Research Participants have the right to object if the Responsible Party is using their Personal Information without POPIA Consent or without a law authorising the Processing.⁷⁷ But the research participant must demonstrate that they have reasonable grounds for the objection.
 - 4.3.9.5.2. If the Responsible Party receives a valid objection, the researcher must stop Processing the Personal Information of Research Participants and must restrict access to their Personal Information.⁷⁸

- 4.3.9.6. The right to access their own personal information when PAIA permits it
 - 4.3.9.6.1. Research Participants have the right to receive confirmation that their Personal Information is being used in Research and to access a record of their Personal Information.⁷⁹
 - 4.3.9.6.2. The right of Research Participants to access their Personal Information is not absolute. For instance, they are not entitled to their own Personal Information if giving access would:⁸⁰
 - 4.3.9.6.2.1. reveal the Personal Information of someone else without their permission;⁸¹
 - 4.3.9.6.2.2. cause serious harm to the Research Participant's physical or mental health, and the Research Participant has not made arrangements for counselling;⁸²
 - 4.3.9.6.2.3. expose the Research to serious disadvantage; ⁸³or
 - 4.3.9.6.2.4. compromise someone else's intellectual property or confidential information.⁸⁴
- 4.3.9.7. The right to correct or delete their personal information
 - 4.3.9.7.1. Research Participants can ask that researchers correct Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete or misleading.⁸⁵
 - 4.3.9.7.2. When researchers receive such a request, they must either:⁸⁶
 - 4.3.9.7.2.1. correct or delete the Personal Information; or
 - 4.3.9.7.2.2. provide credible evidence to the satisfaction of the research participant that the Personal Information is correct (in the interim, the Personal Information must be restricted).
 - 4.3.9.7.3. If the researcher and Research Participant cannot agree on the accuracy of the Personal Information, researchers must indicate in their records that there is a dispute about the accuracy of the Personal Information.⁸⁷

4.3.9.7.4. If the researcher agrees that the Personal Information should be corrected or deleted and if correcting or deleting the Personal Information has an impact on decisions that have been or will be taken about the Research Participants, the researcher must inform everybody to whom the Personal Information was provided about the correction or deletion.⁸⁸

4.3.9.8. The right to make representations about automated decisions with a legal or substantial effect

4.3.9.8.1. Research Participants have additional rights if Research involves automated decision-making. Automated decisions are decisions that:⁸⁹

4.3.9.8.1.1. have legal consequences or will have a substantial effect on the Research Participant (e.g., whether they will receive medical treatment or not);

4.3.9.8.1.2. are automated (i.e., made without human intervention); and

4.3.9.8.1.3. are based on an analysis of aspects of a research participant's personality, behaviour, interests, and habits (e.g., performance at work, creditworthiness, reliability, location, health, personal preferences, or conduct).

4.3.9.8.2. When Research involves automated decision-making, researchers must:⁹⁰

4.3.9.8.2.1. give Research Participants an opportunity to make representations about that decision; and

4.3.9.8.2.2. provide Research Participants with sufficient information about the underlying logic of the automated decision to allow Research Participants to make representations.

4.3.10. Transborder information flows

4.3.10.1. Research activities often require that Personal Information must be

transferred to other countries. To comply with this Code, the transfer must meet one of the following requirements:⁹¹

- 4.3.10.1.1. The country must have laws that are equivalent to POPIA. The Code considers countries in the European Union or a country that has received an [adequacy decision from the European Commission, as equivalent to POPIA](#).
- 4.3.10.1.2. If the recipient is a co-Responsible Party, the Responsible Party must have concluded an agreement (e.g., a data transfer agreement) with them that the co-Responsible Party will comply with the Code.
- 4.3.10.1.3. If the recipient is an [operator, the](#) Responsible Party must have concluded an agreement with them that the operator will comply with the [security safeguards](#) section of the Code.
- 4.3.10.1.4. The recipient must be part of the same 'group of undertakings' as the Responsible Party and must be bound by policies that require compliance with the Code.
- 4.3.10.1.5. The Research Participant must have consented to the transfer of Personal Information and there must be a process in place to facilitate the withdrawal of POPIA Consent.
- 4.3.10.1.6. 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.

4.3.11. Information matching programmes⁹²

- 4.3.11.1. Research usually does not constitute 'information matching programmes' as defined in POPIA⁹³ because Research does not result in 'taking any action in regard to an identifiable data subject'.

4.3.12. Implementation and monitoring

- 4.3.12.1. If the Research is high-risk, an Information Officer or Deputy Information Officer, or a senior employee(s) formally designated to perform this task on their behalf, must approve the Research Protocol and monitor

compliance regularly, but at least once every two years.

5. ENFORCEMENT OF THE CODE ⁹⁴

5.1. The following people may submit a complaint to ASSAf:

5.1.1. [Research Participants](#)

5.1.2. a person acting on behalf of a Research Participant

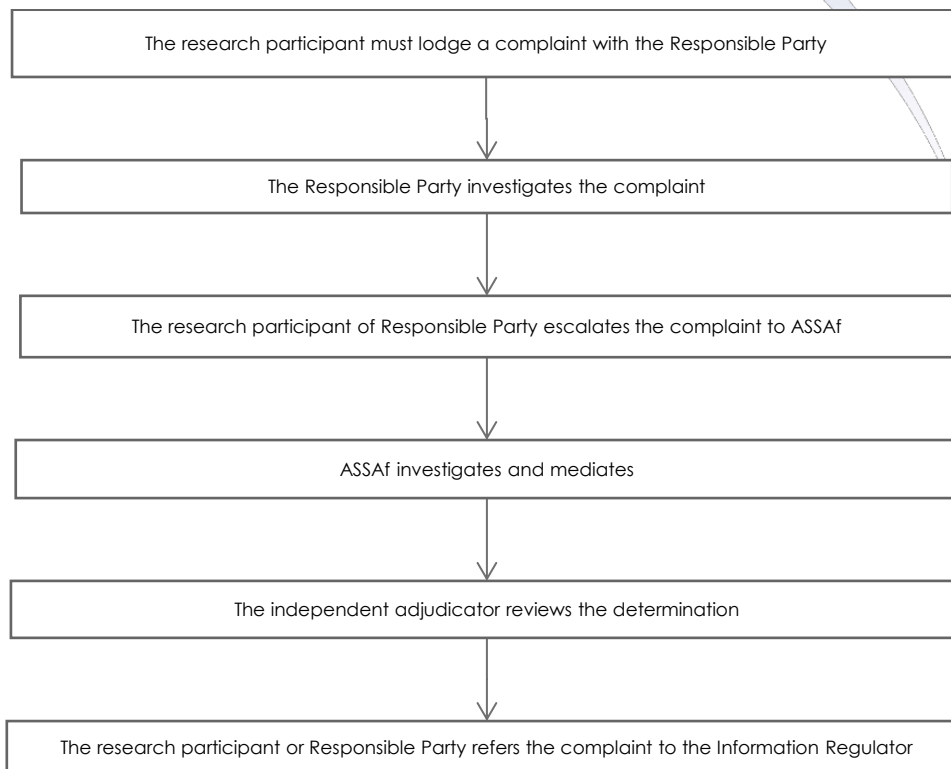
5.1.3. a competent person acting on behalf of a Research Participant who is a [Child](#)

5.1.4. a person appointed by a court to manage the affairs of a Research Participant

5.2. This Code does not cover complaints of non-compliance with the Code where the complainant is a [Responsible Party](#) or a researcher.

5.3. Responsible Parties and ASSAf must follow the following process when they receive a complaint from a Research Participant:

5.3.1. The complaints process



5.3.1.1. The Research Participant must lodge a complaint with the responsible party

5.3.1.1.1. Responsible Parties must:

- 5.3.1.1.1.1. let Research Participants know how to lodge a complaint;
- 5.3.1.1.1.2. use a form that is substantially similar to Part 1 of Form 5;
- 5.3.1.1.1.3. have a dedicated contact person who receives complaints;
- 5.3.1.1.1.4. have a process in place to manage complaints; and
- 5.3.1.1.1.5. help Research Participants to ensure that the complaint is heard – even if Research Participants do not follow the correct procedure.

5.3.1.1.2. If a Research Participant believes that a Responsible Party has breached this Code, they must lodge a complaint with the Responsible Party first for a determination.⁹⁵ If a Research Participant

makes the complaint directly with ASSAf, ASSAf will refer the complaint to the Responsible Party.

5.3.1.1.3. Research Participants or ASSAf may escalate the complaint to the Information Regulator if:

5.3.1.1.3.1. the Research Participant will be disadvantaged if the complaint is directed to the Responsible Party;

5.3.1.1.3.2. a systemic violation of the protection of [Personal Information](#) has occurred;

5.3.1.1.3.3. the Responsible Party has a history of habitual violation of the protection of Personal Information;

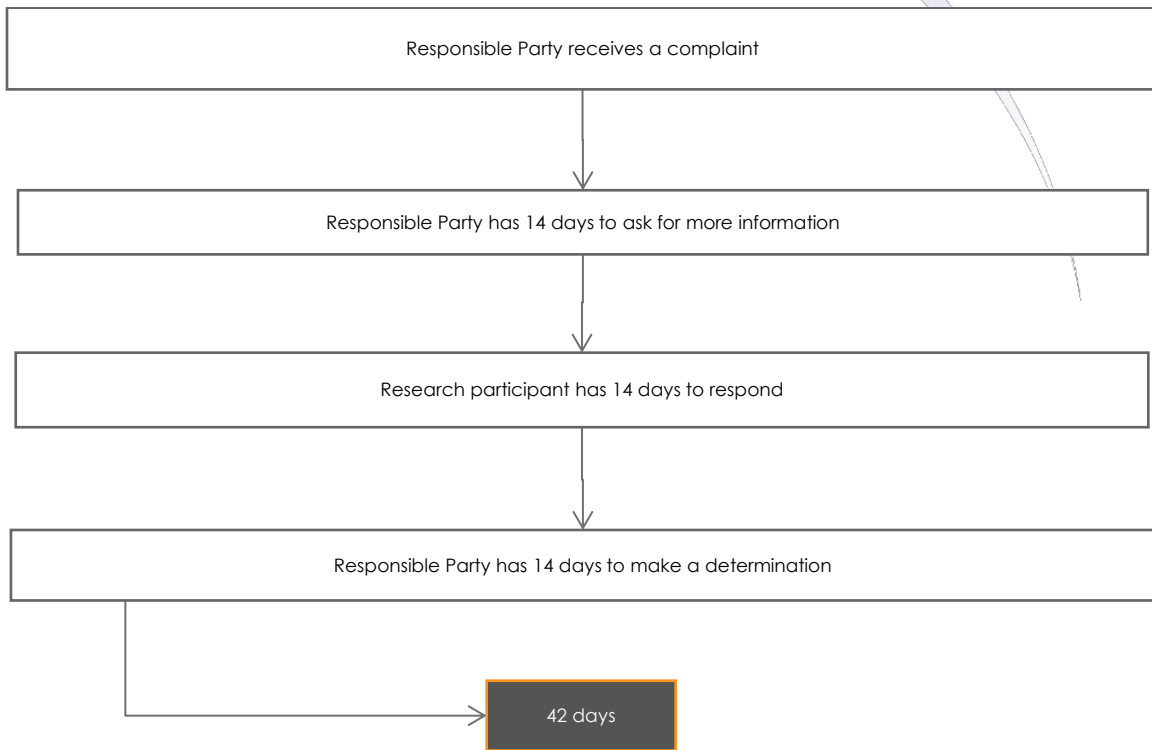
5.3.1.1.3.4. the complainants represent a class of Research Participants who are bringing a complaint against the same Responsible Party; or

5.3.1.1.3.5. several complaints have been received that arose out of similar circumstances, and there is a common issue of law or fact.

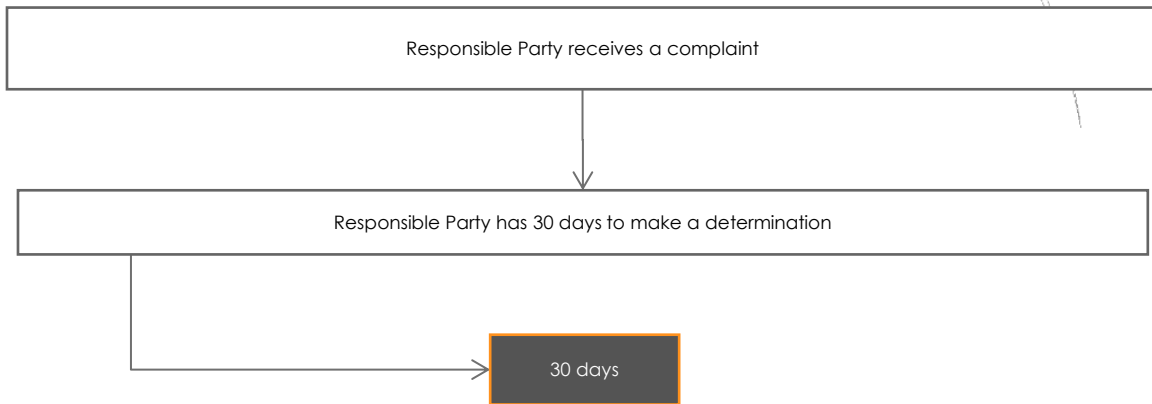
5.3.1.2. [The responsible party investigates the complaint](#)

5.3.1.2.1. If the Responsible Party needs further information to investigate the complaint, they must request it from the Research Participant within 14 calendar days from receiving the complaint.

5.3.1.2.2. The Responsible Party must give the Research Participant at least 14 calendar days to respond to the request for further information. The Responsible Party must make a decision on the information received from the Research Participant within 14 calendar days of the end of the response period. The Responsible Party must provide reasons for their decision in writing and in [Plain Language](#).



5.3.1.2.3. If the Responsible Party does not require further information, they must make a decision within 30 calendar days of receiving the complaint.



- 5.3.1.2.4. The Research Participant or responsible party escalates the complaint to ASSAf
- 5.3.1.2.5. The Research Participant may refer the complaint to ASSAf within 30 calendar days of receiving the Responsible Party's decision.
- 5.3.1.2.6. The Responsible Party must inform the Research Participant of their right to escalate their complaint to ASSAf. The Responsible Party must also provide reasonable assistance to make sure that the Research Participant's complaint reaches ASSAf.
- 5.3.1.2.7. The Research Participant must send the following documentation to **[insert email]**:
 - 5.3.1.2.7.1. The original complaint and any additional information they provided to the Responsible Party;
 - 5.3.1.2.7.2. The decision made by the Responsible Party.
 - 5.3.1.2.7.3. The reasons why the Research Participant does not agree with that decision.

- 5.3.1.2.8. If the Research Participant requests it, the Responsible Party must provide ASSAf with the original complaint, additional information, and determination.
- 5.3.1.3. **ASSAf investigates and mediates**
- 5.3.1.3.1. ASSAf will investigate the complaint and advise the Research Participant of the outcome of the investigation within 30 calendar days of receiving the complaint.
- 5.3.1.3.2. ASSAf representatives may engage directly with the Responsible Party and the Research Participant to try to resolve the complaint.
- 5.3.1.3.3. If the Responsible Party assures ASSAf that they will not repeat the action complained of, and the Research Participant is satisfied, ASSAf may ask that the Information Regulator issue a settlement certificate in terms of section 80.
- 5.3.1.4. **The independent adjudicator reviews the determination**
- 5.3.1.4.1. If ASSAf cannot broker a settlement within 45 calendar days of receiving the complaint, it will refer the complaint to the independent adjudicator and provide them with all the documents the Responsible Party and the Research Participant submitted.
- 5.3.1.4.2. The independent adjudicator may ask the Responsible Party and the Research Participant for more information.
- 5.3.1.4.3. The independent adjudicator must provide ASSAf with a written decision on the complaint within 45 calendar days of receiving the complaint. It may take longer if it is necessary to ask for more information to adjudicate the complaint fairly.
- 5.3.1.4.4. If the adjudicator finds that the Responsible Party is in breach of the Code, ASSAf may ask the Responsible Party to:
- 5.3.1.4.4.1. take specified steps; or
 - 5.3.1.4.4.2. stop [Processing](#) Personal Information for a specified purpose or in a specified manner.

- 5.3.1.4.5. ASSAf will communicate the decision to the Responsible Party within 14 calendar days of receiving the independent adjudicator's decision.
- 5.3.1.5. The Research Participant or responsible party refers the complaint to the information regulator
- 5.3.1.5.1. If the Responsible Party or the Research Participant is not satisfied with the independent adjudicator's decision, they may refer the complaint to the Information Regulator. They can do this by submitting [Part II of Form 5](#) to POPIAcomplaints@inforegulator.org.za within 30 calendar days of receiving the decision.⁹⁶
- 5.3.1.5.2. The decision of the independent adjudicator will remain in effect until the Information Regulator makes a decision.⁹⁷

5.3.2. Independent adjudicator⁹⁸


- 5.3.2.1. Appointment
 - 5.3.2.1.1. ASSAf will appoint five individuals to serve on its panel of independent adjudicators. When ASSAf receives a complaint for adjudication, it will assign an independent adjudicator(s) to make a decision. These assigned adjudicator(s) must not have any conflicts of interest or any affiliation with the Responsible Party or Research Participant.
 - 5.3.2.1.2. The independent adjudicators must have suitable qualifications or experience at an expert level in Research, research data management, research ethics or data protection. They must have an impeccable reputation and must not have been found guilty of research misconduct or ethical violations in the past.
- 5.3.2.2. How independent adjudicators must adjudicate complaints
 - 5.3.2.2.1. The independent adjudicator must:
 - 5.3.2.2.1.1. consider the matters listed in section 44 of [POPIA](#) when adjudicating a complaint;
 - 5.3.2.2.1.2. be impartial;

- 5.3.2.2.1.3. be accessible and efficient;
 - 5.3.2.2.1.4. assist Research Participants to participate in the adjudication process;
 - 5.3.2.2.1.5. follow a flexible procedure; and
 - 5.3.2.2.1.6. observe the principles of natural justice and procedural fairness.
- 5.3.2.2.2. Adjudicators may call for further information or require that the Research Participant or Responsible Party provide oral evidence.
- 5.3.2.3. **Reports to the Information Regulator**
- 5.3.2.3.1. The panel of independent adjudicators must submit an annual report to the Information Regulator that specifies the number and nature of complaints made to an adjudicator during that financial year.
- 5.3.2.3.2. The report must be made in a form that is satisfactory to the Information Regulator within five months of the end of the Information Regulator's financial year (31 March).

6. ADMINISTRATION OF THE CODE

6.1. Monitoring compliance with the Code

- 6.1.1. ASSAf may, of its own accord, or in response to a complaint:
- 6.1.1.1. ask a [Responsible Party](#) to demonstrate that they comply with the Code by producing the documentation referred to in the [accountability checklist](#); or
 - 6.1.1.2. require a Responsible Party to produce a report by an independent auditor that they comply with the Code, at the cost of the Responsible Party.
- 6.1.2. ASSAf will provide an annual report to the Information Regulator that includes:
- 6.1.2.1. the steps ASSAf took to monitor compliance with the Code;
 - 6.1.2.2. information received from Responsible Parties on their level of

- 
- compliance;
- 6.1.2.3. the number and nature of complaints made to an adjudicator during that financial year, the average time it took to resolve the complaints and statistical information about the nature and outcomes of the complaints;
 - 6.1.2.4. aggregate information about systemic issues or serious or repeated non-compliance with the Code; and
 - 6.1.2.5. trends on the effectiveness of the Code.

6.2. Review of the Code

- 6.2.1. The Information Regulator may request a review of the Code at any time.
- 6.2.2. ASSAf will review the Code annually and apply to the Information Regulator to vary the Code to:
 - 6.2.2.1. reflect any changes in [Research](#) practices or technology, or
 - 6.2.2.2. remedy a lack of compliance with the Code.
- 6.2.3. Section 60 to 63 of [POPIA](#) sets out the process which must be followed to vary the Code.

6.3. Expiry of the Code

- 6.3.1. The Code will expire on the 5th anniversary of its effective date.

7. GLOSSARY

Table 11: 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.⁹⁹</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.¹⁰⁰ 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>
Independent Researchers	<p>An individual who is <u>not</u> an 'employee' of a Research Institution in terms of South African labour law.</p> <p>A person is an employee if they meet the definition in the Labour Relations Act 66 of 1995 and the Basic Conditions of Employment Act 75 of 1997.</p>
PAIA	<p>The Promotion of Access to Information Act 2 of 2000 and its regulations.</p>
Personal Information	<p>Personal Information includes any information that relates to an <u>identifiable</u>, living individual or to an identifiable, existing juristic person (e.g., a company or other type of</p>

	<p>organisation).¹⁰¹</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 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 who 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. ¹⁰²
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. ¹⁰³
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: ¹⁰⁴ <ul style="list-style-type: none"> • 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 a power or performing a duty in terms of the Constitution or a provincial institution

	<ul style="list-style-type: none"> any other function or institution that is exercising a public power or performing a public function in terms of any legislation
<p>Research</p>	<p>Research includes the activities that are aimed at improving knowledge of any discipline through enquiry or systematic investigation. This Code 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 Code 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 Code will NOT apply to:</p> <ul style="list-style-type: none"> Profiling individuals to decide whether to market or offer to supply a product or service to that specific individual.¹⁰⁵

	<ul style="list-style-type: none"> • Statistical analysis.¹⁰⁶
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 Institutions	<p>An institution (e.g., a company, university or any other private or Public Body) that conducts Research.</p> <p>An entity acting through its employees is vicariously liable for the actions of those employees, provided that the employee is acting within the course and scope of their employment. A person is an employee if they meet the definition in the Labour Relations Act 66 of 1995 and the Basic Conditions of Employment Act 75 of 1997.</p>
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 Code.</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)	<p>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 Processing Personal Information'.¹⁰⁷ The Responsible Party is the private or Public Body(s) or any person(s) who determines why and how Personal Information is Processed.¹⁰⁸ In most instances, the private or Public Body that employs, or directly controls the researchers will be the Responsible Party. The</p>

	<p>researchers will only be Responsible Parties in their individual capacity if the Responsible Party (private or Public Body) does not employ or control them; in other words if they are Independent Researchers.</p>
Research Protocol	<p>Research Protocol is documentation that outlines the plan of a research study (e.g., data management plans or similar documents).</p>
Special Personal Information	<p>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.</p> <p>The following list contains examples of what Special Personal Information of Research Participants typically is:</p> <ul style="list-style-type: none"> • 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

	<p>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.</p> <ul style="list-style-type: none"> • Sex life: E.g., 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.)
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).

Annexure A: When personal information is identifiable

1. When personal information is identifiable

1.1. [POPIA](#), and therefore the Code, does not apply if [Personal Information](#) has been permanently de-identified.¹⁰⁹

1.2. De-identification means to delete Personal Information that:

1.2.1. identifies [Research Participants](#);

1.2.2. can be manipulated to identify Research Participants; or

1.2.3. can be linked by a reasonably foreseeable method to other information that identifies Research Participants.¹¹⁰

1.3. The Code acknowledges that complete de-identification or anonymisation is difficult, if not impossible, to achieve, considering technological advancements and the fact that increasing volumes of Personal Information are in the public domain.


1.4. Here are some examples of identifiers which, if collected or obtained, would identify a Research Participant or make them identifiable:¹¹¹

1.4.1. name;

1.4.2. identification number (e.g., an ID number, passport number, staff number, student number, participant identification number, patient number or other reference numbers which uniquely identify the Research Participant);

1.4.3. online identifier;

1.4.4. telephone number;

- 
- 1.4.5. email address; or
 - 1.4.6. any additional Personal Information that directly identifies the Research Participant.
 - 1.5. [Biometric](#) information, including genetic data is only considered identifiable if it is linked through specific technical processing to other Personal Information that can directly or indirectly identify a living individual.
 - 1.6. Even when no identifiers are collected, the Research Participant may still be identifiable through manipulation or linking. To determine whether the Research Participant is identifiable, researchers must consider:¹¹²
 - 1.6.1. how the [Research Institutions](#), [Independent Researchers](#) or another person could identify the Research Participant;
 - 1.6.2. the cost of re-identification;
 - 1.6.3. the amount of time required for re-identification;
 - 1.6.4. the available technology at the time and technological developments that are already at an advanced stage;
 - 1.6.5. the environment in which the researchers will store the Personal Information (e.g., access controls, restrictions on data sharing or anonymisation techniques to prevent re-identification); and
 - 1.6.6. additional information that might be available for linking and who has access to that information.
 - 1.7. [Research Institutions](#) or [Independent Researchers](#) should adopt the 'motivated intruder test'. This test is used as a standard for determining whether there is a high risk of re-identification, whether an intruder would be able to achieve identification if they were motivated to attempt it. The following documents contain guidelines on how to apply the test:
 - 1.7.1. [ICO 'Draft anonymisation, pseudonymisation and privacy-enhancing](#)

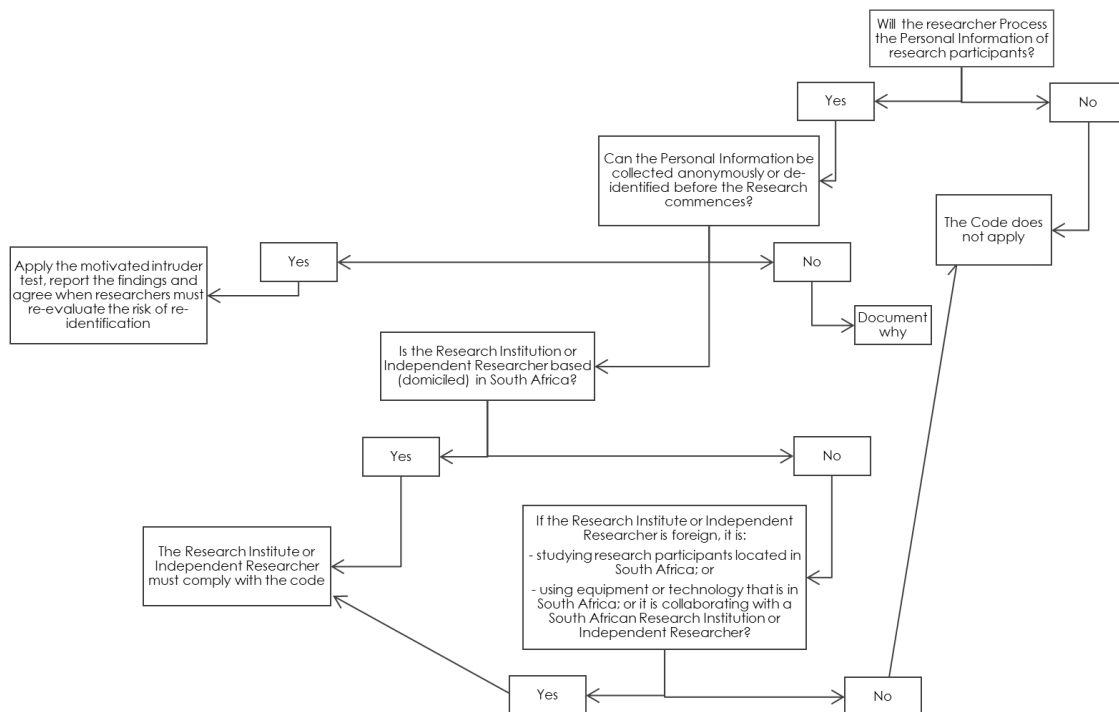
[technologies guidance: Chapter 2'](#)

- 1.7.2. [Irish Data Protection Commission' Guidance on Anonymisation and Pseudonymisation'](#)
- 1.7.3. [The Commonwealth Scientific and Industrial Research Organisation \(Australia\) 'The De-Identification Decision-Making Framework'](#)
- 1.8. For guidance on different anonymisation techniques and their effectiveness, also see the [Article 29 Working Group' Opinion 05/2014 on Anonymisation Techniques'](#)
- 1.9. Responsible parties must:
 - 1.9.1. develop and implement an assessment to measure the risk of re-identification;
 - 1.9.2. document to what extent the Personal Information has been de-identified; and
 - 1.9.3. 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.
- 1.10. If the risk of re-identification is low, POPIA and this Code will not apply.

Annexure B: Screening assessment

1. A screening assessment

1.1. Ask these questions to determine whether the Code applies to a Research activity (e.g., a project or study):



Annexure C: Minimality assessment

1. Use these questions to assess whether the [Processing](#) of identifiable [Personal Information](#) is necessary and proportional.

Questions to assess whether the processing of identifiable personal information is necessary and proportional

The question	Guidance on interpreting the answer
Is it necessary to collect all the Personal Information?	<p>Researchers should not collect Personal Information that is not necessary to achieve the purpose of the Research.</p> <p>It is possible to collect Personal Information for future use, and the Code recognises that it may not always be possible to foresee what Personal Information the researchers (or future researchers) will require. When this is the case, the researcher must document potential future uses as accurately as possible.</p>
Is there a less intrusive way to Process the Personal Information?	<p>Researchers must investigate and determine the least intrusive way to Process the Personal Information. E.g., Pseudonymisation.</p> <p>In high-risk Research, researchers must Pseudonymise Personal Information to</p>

limit the number of people who have access to the identities [of Research Participants](#). If Pseudonymisation is not possible, the researcher must document why. If the Personal Information is shared with [Third Parties](#), it must be Pseudonymised, and the agreement must prohibit re-identification.

The following documents contain guidelines on Pseudonymisation:

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

Annexure D: Records retention

1. Responsible Parties should retain the following information about [Research](#) activities:

Table 1: Responsible Parties should retain the following information about research activities

Type of record	What must be retained
Research administration information	<p>Documents and information relating to the administration of the Research, including:</p> <ul style="list-style-type: none">• Research Protocols• research ethics approval applications• correspondence between researchers and approval bodies (e.g., feedback from research ethics committees or advice from deputy information officers)• research-related contracts• disclosures made to Research Participants (e.g., information sheets)• POPIA Consent (when obtained) or Research Consent (when obtained) provided by Research Participants (including the procedure and documentation)

Type of record	What must be retained
	<p>used)</p> <ul style="list-style-type: none"> • progress or other reports
<p>Identifiable Personal Information of Research Participants</p>	<p>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 keep the following metadata:</p> <ul style="list-style-type: none"> • 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 start date) • what disclosures were made to the Research Participant (including a reference to the notification documentation) • whether the Research Participant provided a POPIA Consent (including a reference to the consent documentation) • under which conditions the Personal Information can be

Type of record	What must be retained
	<p>shared with external institutions or researchers</p> <ul style="list-style-type: none"> • what the Personal Information can be reused for in future
Anonymised research data	<p>Any Personal Information collected from Research Participants that are no longer identifiable.</p> <p>A log containing the following metadata:</p> <ul style="list-style-type: none"> • when the Personal Information was anonymised • how the Personal Information was anonymised • what the risk of re-identification is • under which conditions it can be shared on open access platforms

2. Responsible Parties should create a research records retention schedule that determines default rules for these categories of records:
 - 2.1. when the record is created (e.g., when the Research is concluded, when POPIA Consent is obtained, when the Research Protocol is approved);
 - 2.2. how long the record should be retained (e.g., indefinitely, at the conclusion of the Research + 10 years);
 - 2.3. why the record must be retained (e.g., for proof; to comply with paragraphs 13.1 and 13.2 of the HPCSA: General ethical guidelines for health researchers).

3. If researchers must deviate from these default rules, this must be recorded in the research proposal.
4. If Personal Information is held in the cloud or by a service provider, the [Responsible Party](#) must ensure that it is securely deleted 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 the Personal Information and for the subsequent re-use of the Personal Information (see the section on further [Processing](#)).

¹ Section 3 of the Academy of Science of South Africa Act 67 of 2001.

² Section 3(2)(a) of POPIA.

³ Section 68.

⁴ The definition of Research is a combination of the Department of Health's, *Health Research: Principles, Processes and Structures* 2nd Edition (2015) and recital 159 of the EU GDPR. Since research is listed as being in the public interest (section 37(2)(e) of POPIA, it is not useful to make this part of the definition.

⁵ Responsible Parties are domiciled in South Africa if they meet the definition of 'resident' in section 1 of the Income Tax Act, 58 of 1962. This will be the case if the Responsible Party is incorporated, established or formed in South Africa, or if it has its 'central management and control' in South Africa.

⁶ The question is whether the foreign Research Institution or Independent Researcher is making use of 'means' in South Africa (see section 3(1)(b) of POPIA). Automated means is defined in section 3(4) as equipment. We took how 'equipment' was interpreted in terms of article 4(1)(c) the European Union Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the Processing of personal data and on the free movement of such data *Official Journal L 281, 23/11/1995*), into account. However, POPIA's automated or non-automated means are broader. The Code goes even further to include the provision that the Code will apply if the research participants are in South Africa, even if the Research Institution or Independent Researcher is not making use of other 'means' in South Africa.

⁷ Section 8 of POPIA states that the Responsible Party must ensure that the conditions are met. Except for sections 20 and 21, the conditions all refer to the 'Responsible Party'.

⁸ See Condition 1: Accountability (section 8) of POPIA.

⁹ Section 1 of POPIA.

¹⁰ In this table we have included the terminology used in the EU GDPR because South African Research Institutions may encounter these terms in contracts with collaborators in the EU and the commentary to the EU GDPR and the Data Protection Directive is useful,

because the concepts are very similar.

¹¹ The definition of Responsible Party in section 1 of POPIA explicitly allows for multiple Responsible Parties acting together.

¹² POPIA is not clear on how liability will be apportioned. Commentary under the EU Data Protection Directive states that unless the co-Responsible Parties or the factual circumstances indicate otherwise, the liability will be joint and several. Please see Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor', 24, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

¹³ See Condition 3: Purpose Specification (section 13) of POPIA.

¹⁴ Section 13(1).

¹⁵ 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.

¹⁶ See article 35(1) of the EU GDPR which outlines when a data protection impact assessment must be conducted. POPIA does not contain a similar provision; it just prescribes that Personal Information impact assessments (PIIAs) must be performed. The risk-based approach proposed here complies with section 44(1)(b) of POPIA, because it balances the public's interest in Research against Research Participants' right to privacy. It also complies with section 9(b) as it ensures reasonableness.

¹⁷ 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.

¹⁸ Section 9 of POPIA.

¹⁹ Section 10.

²⁰ 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).

²¹ In this regard, POPIA is very similar to the EU GDPR. 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_reply_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).

²² Sections 11(1)(b) has been omitted. In general, there will be no contract between the Responsible Party and a Research Participant and therefore section 11(1)(b) will never apply.

²³ Section 11(1)(a).

²⁴ 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.

²⁵ See the definition of consent in section 1 of POPIA.

²⁶ Section 11(1)(c).

²⁷ Section 11(1)(e).

²⁸ Section 11(3)(a).

²⁹ Section 11(3)(f).

³⁰ 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. See the discussion on reasonableness on page 16 of the SA Law Reform Commission *Project 124 on Privacy and Data Protection (2009 Report)*.

³¹ Section 11(3)(a).

³² POPIA does not require a legitimate interest assessment. However, section 36 of the Constitution would trigger such an assessment given that the Research Participant's right to privacy is being limited. A legitimate interest assessment is a useful way to document that such an assessment was done and aligns the Code with international standards.

³³ Sections 27(1)(b) and (c) have been omitted. These sections state that a Responsible Party can Process Special Personal Information if it is necessary for the establishment, exercise, or defense of a right or obligation in law or to comply with an obligation of international public law. This will rarely, if ever, be the case in respect of Research.

³⁴ Section 27(1)(a).

³⁵ Section 27(1)(d)(i). The requirement that the Processing must be necessary has been omitted because this is always a requirement to comply with the principal of minimal Processing. The requirement that there must be sufficient guarantees in place has been omitted, because adherence to an approved Code of Conduct is an example of such a guarantee (see recital 81 and article 28(1), (4) and (5) of the EU GDPR).

³⁶ Information Regulator *Guidance Note on Processing of Special Personal Information*, available at <https://www.justice.gov.za/infoereg/docs/InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628.pdf> (last accessed on 30 March 2022).

Also see Donrich Thaldar 'Research and the meaning of "public interest" in POPIA' *South African Journal of Science* (2022) 118(3/4)

³⁷ Section 27(1)(d)(ii). The requirement that there must be sufficient guarantees in place has been omitted, because adherence to an approved Code of Conduct is an example of such a guarantee (see recital 81 and article 28(1), (4) and (5) of the EU GDPR).

³⁸ This interpretation is consistent with how similar provisions have been interpreted in the courts in the EU and New Zealand.

³⁹ Section 27(1)(e).

⁴⁰ 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).

⁴¹ They have been omitted here because it is unlikely that they will apply to Research.

⁴² Sections 35(1)(b) and (c) have been omitted. These sections state that a Responsible Party can Process a Child's Personal Information if it is necessary for the establishment, exercise, or defense of a right or obligation in law or to comply with an obligation of international public law. This will rarely, if ever, be the case in respect of Research.

⁴³ Section 1 of POPIA.

⁴⁴ Section 35(1)(a).

⁴⁵ The definition of 'Child' and 'competent person' in section 1. Parental responsibilities are conferred in terms of the Children's Act 38 of 2005.

⁴⁶ Section 35(1)(d)(i). The requirement that the Processing must be necessary has been omitted because this is always a requirement to comply with the principle of minimal Processing. The requirement that there must be sufficient guarantees in place has been omitted, because adherence to an approved Code of Conduct is an example of such a guarantee (see recital 81 and article 28(1), (4) and (5) of the EU GDPR).

⁴⁷ This definition of public interest is adapted from the Information Regulator's *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).

⁴⁸ Section 35(1)(d)(ii). The requirement that there must be sufficient guarantees in place has been omitted, because adherence to an approved Code of Conduct is an example of such a guarantee (see recital 81 and article 28(1), (4) and (5) of the EU GDPR).

⁴⁹ This interpretation is consistent with how similar provisions have been interpreted in the courts in the EU and New Zealand.

⁵⁰ Section 35(1)(e).

⁵¹ 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://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 30 March 2022).

⁵² Section 12(1).

⁵³ Section 12(2)(d)(i) to (iv) have been omitted intentionally, because they can apply to Public Bodies who are involved in the detection, investigation, prosecution, and punishment of offences; SARS; courts or tribunals; or where Processing is in the interests of national security. These justifications will rarely if ever apply to Research.

⁵⁴ Section 12(2)(a).

⁵⁵ The definition of public record in section 1.

⁵⁶ The definition of 'Public Body' in section 1.

⁵⁷ Section 12(2)(a).

⁵⁸ Section 12(2)(b).

⁵⁹ Section 12(2)(c).

⁶⁰ Section 12(2)(d)(v).

⁶¹ Section 12(2)(e).

⁶² Section 12(2)(f).

⁶³ Section 14.

⁶⁴ Section 14(6)(b).

⁶⁵ Section 14(2). The section requires that there must be 'satisfactory safeguards' in place

to ensure that the Personal Information is only used for research purposes. This Code constitutes such a safeguard.

⁶⁶ Section 15(3)(c) and (f) have been omitted as they will rarely if ever, apply in this context.

⁶⁷ See sections 10 and 16.

⁶⁸ These steps are derived from European Data Protection Board *Guidelines 4/2019 on Article 25 Data Protection by Design and Default* from page 23

(https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf),

⁶⁹ Section 23(1).

⁷⁰ Researchers will not be able to use algorithms that make automated decisions that can have a substantial effect on Research Participants unless the Code contains 'appropriate measures...for protecting the legitimate interests' of Research Participants. See section 71(3)(b).

⁷¹ Section 17.

⁷² Regulation 4(1)(a) of the POPIA Regulations.

⁷³ Section 18(4)(f)(ii).

⁷⁴ 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).

⁷⁵ Section 22(1).

⁷⁶ Section 11(2)(b).

⁷⁷ Section 11(3)(a).

⁷⁸ Section 11(4) read with section 14(6)(b).

⁷⁹ Section 23(1)(a) and (b).

⁸⁰ PAIA contains several grounds on which access can be denied. It was not practical to list them all here, but the most common grounds are listed as examples.

⁸¹ Section 34 or 63 of PAIA.

⁸² Section 30 and 61 of PAIA.

⁸³ Section 43 and 69 of PAIA.

⁸⁴ Sections 36, 37, 42, 64, 65 and 68 of PAIA..

⁸⁵ Section 24(1).

⁸⁶ Section 24(2)(a) to (c) read with section 14(6)(a).

⁸⁷ Section 24(2)(d).

⁸⁸ Section 24(3).

⁸⁹ Section 71(1). Also see article 4(4) of the GDPR.

⁹⁰ Section 71(2)(b) and 71(3).

⁹¹ Section 72(1).

⁹² Codes are required to contain a section on information matching programmes. It is defined in section 1 of POPIA. In the case of research, information matching programmes are not a concern. The Code is required to state this.

⁹³ Section 1.

⁹⁴ The previous draft of the Code provided that Responsible Parties could approach ASSAf for advice or make complaints against other Responsible Parties. This is not referred to in POPIA. It was included because it appeared in the Credit Bureau Association's Code. It has been left out because it will place an additional burden on ASSAf.

⁹⁵ Section 77(1)(f) provides that the Information Regulator can decline to act if the Research Participant does not follow the complaints procedure set out in an accredited Code.

⁹⁶ Section 63(3).

⁹⁷ Section 63(4).

⁹⁸ The previous draft of the Code copied the extensive provisions of the draft CBA code on the appointment of adjudicators. This is not required by POPIA. The [Guidelines to develop Codes of Conduct](#) provides that ASSAf must appoint the independent adjudicator and that the Code must provide for the details of the independent adjudicator.

⁹⁹ Section 1.

¹⁰⁰ Section 1.

¹⁰¹ Section 1.

¹⁰² This definition has been adapted from section 22 of the Consumer Protection Act 68 of 2008.

¹⁰³ Section 1.

¹⁰⁴ Section 1.

¹⁰⁵ This activity is excluded from the Code 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.

¹⁰⁶ Statistical analysis that is done on anonymous or aggregated information is not subject to the Code, because it does not involve identifiable Personal Information.

¹⁰⁷ Section 1 of POPIA.

¹⁰⁸ Section 1 of POPIA.

¹⁰⁹ Section 6(1)(b) of POPIA.

¹¹⁰ The definition of 'de-identify' in section 1 of POPIA.

¹¹¹ This list is derived from the definition of unique identifier in section 1 of POPIA, the Information Regulator's examples of unique identifier in paragraph 3.1.1 of its *Guidance note on applications for prior authorisation*, available at <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PriorAuthorisation-20210311.pdf> (last accessed on 31 March 2022) and article 4(1) of the EU GDPR.

¹¹² These factors are listed in recital 26 of the EU GDPR.