



USAF POPIA GUIDELINE



TABLE OF CONTENTS

1.	INTRODUCTION	4
1.1.	BACKGROUND	4
1.2.	SCOPE OF THIS GUIDELINE	4
1.3.	PURPOSE OF THIS GUIDELINE	4
1.4.	STATUS OF THIS GUIDELINE	5
1.5.	INTERACTION WITH EXISTING LEGISLATION, CODES, AND GUIDELINES	5
2.	WHEN POPIA APPLIES	7
2.1.	HOW TO DETERMINE WHEN POPIA APPLIES	7
2.2.	INSTITUTIONS MAY APPLY FOR AN EXEMPTION FROM POPIA	12
3.	WHO IS RESPONSIBLE FOR POPIA COMPLIANCE.....	14
3.1.	HOW TO IDENTIFY RESPONSIBLE PARTIES AND OPERATORS	14
3.2.	ACCOUNTABILITY OF RESPONSIBLE PARTIES	17
4.	HOW TO ASSESS COMPLIANCE	19
4.1.	RESPONSIBLE PARTIES MUST ASSESS POPIA COMPLIANCE	19
4.2.	INSTITUTIONS MUST RECORD THEIR PROCESSING ACTIVITIES	22
4.3.	INSTITUTIONS MUST DETERMINE AND DOCUMENT THE PURPOSE FOR PROCESSING PERSONAL INFORMATION	23
4.4.	INSTITUTIONS MUST KEEP PROCESSING TO A MINIMUM	23
4.5.	INSTITUTIONS MUST HAVE A LEGAL BASIS FOR PROCESSING	24
4.6.	INSTITUTIONS MUST COLLECT PERSONAL INFORMATION FROM THE DATA SUBJECT	54
4.7.	INSTITUTIONS MUST NOTIFY DATA SUBJECTS OF PROCESSING	56
4.8.	INSTITUTIONS MUST ENSURE THE QUALITY OF PERSONAL INFORMATION.....	61
4.9.	INSTITUTIONS MUST ENSURE THE SECURITY OF PERSONAL INFORMATION	64
4.10.	USING AN OPERATOR TO PROCESS PERSONAL INFORMATION ON AN INSTITUTION'S BEHALF	67
4.11.	WHEN INSTITUTIONS MUST DELETE OR DESTROY PERSONAL INFORMATION	68
4.12.	WHEN INSTITUTIONS MUST RESTRICT THE PROCESSING OF PERSONAL INFORMATION.....	70
4.13.	HOW INSTITUTIONS MUST RESPECT DATA SUBJECT RIGHTS.....	71
5.	HOW TO ASSESS POPIA COMPLIANCE OF SPECIFIC PROCESSING ACTIVITIES	76
5.1.	HOW TO ASSESS COMPLIANCE WHEN SHARING PERSONAL INFORMATION	76
5.2.	HOW TO ASSESS COMPLIANCE OF DIRECT MARKETING	83

5.3.	HOW TO ASSESS COMPLIANCE OF AN INFORMATION MATCHING PROGRAMME ..	87
6.	POPIA COMPLIANCE PROGRAMMES	89
6.1.	THE ELEMENTS OF A POPIA COMPLIANCE FRAMEWORK	89
6.2.	HOW TO MANAGE CHANGE	91
6.3.	HOW TO GET EXECUTIVE SPONSORSHIP	92
6.4.	HOW TO CONSULT WITH STAKEHOLDERS	93
6.5.	HOW TO DEFINE ROLES AND RESPONSIBILITIES	96
6.6.	WHICH POLICIES TO DEVELOP	98
6.7.	HOW TO IMPLEMENT POLICIES	102
6.8.	HOW TO DO PERSONAL INFORMATION IMPACT ASSESSMENTS	105
6.9.	HOW TO MONITOR AND CONTINUALLY IMPROVE COMPLIANCE	108
6.10.	HOW TO PREPARE FOR AN ASSESSMENT FROM THE REGULATOR	108
7.	GLOSSARY	109

TABLE OF FIGURES

Figure 1: The information lifecycle	11
Figure 2: Questions institutions must answer to identify responsible parties and operators.....	16
Figure 3: Risk management process.....	20
Figure 4: Appropriate legal justification for each piece of personal information	26
Figure 5: How institutions may apply for prior authorisation.....	53
Figure 6: POPIA compliance framework	91
Figure 7: Functional areas within an institution	95
Figure 8: Assessing the impact of the POPIA compliance programme on each stakeholder	96
Figure 9: The role of the three lines of defence in POPIA compliance.....	97
Figure 10: Questions institutions should ask to develop a policy implementation plan.....	103

What the different blocks in this Guideline mean:

	Sections of POPIA that apply.
	Definitions. There are more definitions in the glossary .
	Recommendations. These are not required according to POPIA, but they are best practice.
	Examples.

1. INTRODUCTION

This section discusses the background of this Guideline, the scope, purpose and status of the Guideline, and the interaction of the Guideline with existing legislation, codes and other guidelines.

1.1. BACKGROUND

Universities South Africa ('USAf') is a membership organisation that represents public universities in South Africa. It aims to promote a more inclusive, responsive and equitable national system of higher education. In July and August 2019, USAf held national consultative workshops with University Registrars, IT Directors, Research Directors, and other relevant stakeholders. During these workshops, USAf took the view that public universities should adopt a sector guideline for the Protection of Personal Information Act (POPIA) to help the sector comply with POPIA's requirements.

USAf published the first edition of these guidelines in September 2020. POPIA came into full effect on 1 July 2021, and the Information Regulator (the 'Regulator') has issued several guidance notes, tools, and enforcement notices since then. This second edition of the USAf guidelines builds upon the first by capturing advancements in global leading practices and contextualising the additional materials released by the Regulator.

1.2. SCOPE OF THIS GUIDELINE

This Guideline applies to all processing of personal information by 'public higher education institutions' as defined in section 1 of the Higher Education Act, 101 of 1977.

The Guideline does not address compliance with POPIA when institutions, their staff and students process personal information in a research context. The application of POPIA to research activities will be addressed by the Academy of Science of South Africa (Assaf) in their POPIA Compliance Standard.

1.3. PURPOSE OF THIS GUIDELINE

The purpose of this Guideline is to:

- clarify the requirements of POPIA;
- apply POPIA's principles to the industry in such a way that they empower the relevant institutions to ensure compliance;

- increase the level of POPIA compliance in the industry by aligning the industry's approach to privacy protection with that of the Regulator;
- ensure that POPIA is implemented in a uniform and industry-appropriate way by assisting public universities to comply with POPIA and to promote good information and technology governance; and
- provide for the responsible use of personal information within the industry.

1.4. STATUS OF THIS GUIDELINE

Adopting this Guideline is voluntary as it only indicates what public universities could do to become POPIA compliant, not what they must do.

1.5. INTERACTION WITH EXISTING LEGISLATION, CODES, AND GUIDELINES

This Guideline is based on the provisions of POPIA. Within this context, it is important to consider that apart from POPIA, various other pieces of legislation affect the way that public universities process personal information. Here is a non-exhaustive list of such legislation:

- the Constitution of South Africa¹
- the Higher Education Act²
- Regulations for reporting by Public Higher Education Institutions (2014)³
- the National Qualifications Framework Act⁴
- the Continuing Education and Training Act⁵
- the Skills Development Act⁶
- the National Health Act⁷
- South African Ethics in Health Research Guidelines⁸
- the Consumer Protection Act⁹

¹ The Constitution of the Republic of South Africa, 1996.

² No 101 of 1997.

³ No 101 of 1997.

⁴ No 67 of 2008.

⁵ No 16 of 2006.

⁶ No 97 of 1998.

⁷ No 61 of 2003.

⁸ Ethics in Health Research Guidelines, third edition 2024.

⁹ No 68 of 2008.

- the National Credit Act¹⁰
- the Close Corporations Act¹¹
- the Compensation for Occupational Injuries and Diseases Act¹²
- the Copyright Act¹³
- the Promotion of Access to Information Act¹⁴
- the Electronic Communications Act¹⁵
- the Electronic Communication and Transaction Act¹⁶
- the Employment Equity Act¹⁷
- the Labour Relations Act¹⁸
- the Income Tax Act¹⁹
- the Intellectual Property Rights from Publicly Finances Research and Development Act²⁰
- the Basic Conditions of Employment Act²¹
- the Broad-based Black Economic Empowerment Act²²
- the National Archives and Records Services of South Africa²³
- the Promotion of Administrative Justice Act²⁴

¹⁰ No 34 of 2005.

¹¹ No 69 of 1984.

¹² No 130 of 1993.

¹³ No 98 of 1978.

¹⁴ No 2 of 2000.

¹⁵ No 25 of 2002.

¹⁶ No 25 of 2002.

¹⁷ No 55 of 1998.

¹⁸ No 66 of 1995.

¹⁹ No 58 of 1962.

²⁰ No 51 of 2008.

²¹ No 75 of 1997.

²² No 53 of 2003.

²³ No 43 of 1996.

²⁴ No 3 of 2000.



Section 3(2) (Application and interpretation of POPIA)

When an institution applies POPIA and finds a material inconsistency between POPIA and other legislation, the legislation that provides the most extensive protection will be the one that applies. If that is POPIA, then POPIA applies; however, if another act provides more extensive protection than POPIA, that legislation will apply.²⁵ For example:

- If legislation requires that personal information must be processed (such as the National Credit Act²⁶ which requires that certain personal information must be collected), then institutions must comply with that legislation in addition to POPIA.
- If legislation contains a provision that mandates that a particular type of personal information (e.g., employment records) must be kept for a specific period, that legislation will apply. The institution must, however, still comply with the rest of POPIA.
- If legislation is silent on the processing of personal information, POPIA will apply.
- If legislation provides more extensive protection (e.g., the Constitution provides that no person can be forced to participate in scientific research without their consent), that extensive protection must be applied.

2. WHEN POPIA APPLIES

This section sets out how a responsible party can establish if POPIA applies to their activities. It also explains important concepts of POPIA and when a responsible party may apply for an exemption from POPIA.

2.1. HOW TO DETERMINE WHEN POPIA APPLIES



Section 3 (Application and interpretation of the Act)

Section 6 (Exclusions)

The definitions of '[personal information](#)', '[data subject](#)', '[record](#)', '[responsible party](#)' and '[processing](#)' are key in determining which of a public university's activities will be affected by this Guideline.

POPIA applies to all processing of personal information that a responsible party enters into a record in South Africa. Institutions can use the following questions to establish whether POPIA applies to their activities:

²⁵ Section 3(2)(b) of the POPIA.

²⁶ No 34 of 2005.

- Does the institution 'process' 'personal information'?
- Does the institution enter the 'personal information' into a 'record' that forms part of a filing system?
- Is the institution (who is the 'responsible party') domiciled in South Africa? Or is the institution making use of 'automated or non-automated means' to process personal information in South Africa?

2.1.1. Is the institution processing personal information?

To answer this question, institutions must identify personal information and activities where it is being processed.

2.1.1.1. What is 'personal information'?



| Section 1 (Definition of data subject, de-identify and personal information)

[Personal information](#) is all information that can be linked to an identifiable living individual or existing juristic person, such as a company or government institution.

The individual or juristic person to whom personal information relates is the [data subject](#). In your institution, data subjects include students, prospective students, employees, job applicants, research subjects, researchers, council members, authors, committee members, exchange students, post-doctoral fellows, service providers, suppliers, partners, alumni, visitors, members of the public and donors.

Examples of personal information include:

 Type	Examples
Identifiers	A name, identity number, staff number, student number, account number, customer number, company registration number, tax number, IP address, a phone's IMEI number and usernames on websites and social media
Biometric information	Blood types, fingerprints, DNA, retinal scans and voice records Important: Biometrics is defined as 'a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition. This means that a photograph, by itself, is not biometric information; there must be some technical processing (i.e., use of facial recognition software) before it is considered to be biometric information

Demographic information	Race, gender, sex, pregnancy, marital status, nationality, ethnicity, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture and language
Contact details and location	Physical and postal addresses, location information, email addresses, telephone numbers and social media handles
Financial information	Bank and other account numbers, statements, account balances, financial records, salary information and credit history
Background information	Educational, financial, employment, medical, criminal and credit history
Behavioural information	Likes, dislikes, preferences, opinions, views, posts on social media, browser history, location information, shopping history and who you associate with
Correspondence	Emails, direct messages, SMSs, letters, video chats and video meetings
Opinions about a data subject	Opinions expressed about an individual or organisation, such as preferences, trade references or reviews

POPIA does not apply when personal information cannot be linked to an identifiable individual or juristic person.²⁷ This means that, if the link between the information and the data subject is severed through a process referred to as de-identification or anonymisation, POPIA no longer applies.

Information is considered to have been **de-identified** if:

²⁷ See the judgment of the European General Court of 26 April 2023 (ECLI:EU:T:2023:2019) where the ECJ ruled that no personal data is at hand if, for the entity processing the data, it is practically impossible to identify an individual because it would require a disproportionate effort in terms of time, cost and manpower. Ultimately, the ECJ applied a risk-based approach and assumed data is anonymous if the risk of identification "appears in reality to be insignificant".

- the data subject cannot be identified directly from the information;
- all information that can be used or manipulated by a reasonably foreseeable method to identify the data subject has been deleted; or
- it is impossible to re-identify the information by linking it to other information (e.g., public information, information held by another institution, or the government).

Personal information may contain direct (e.g., name, ID number) and indirect identifiers (e.g., date of birth, gender, race). When the direct identifiers have been eliminated or transformed, but indirect identifiers remain intact, personal information has been **pseudonymised**. The information will be de-identified only once all direct and indirect identifiers have been removed or manipulated to break the link to real-world identifiers.²⁸



Recommendation:

Institutions should classify information under their control.²⁹ Although information classification is not explicitly required in POPIA, it is an important step in information governance. Distinguishing personal information from other information (e.g., policies, contracts, academic lecture notes, and other intellectual property) is vital to determine when POPIA applies and to achieve POPIA compliance. Institutions should have a process to identify all personal information in its possession or under its control.

2.1.1.2. What is processing?



Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

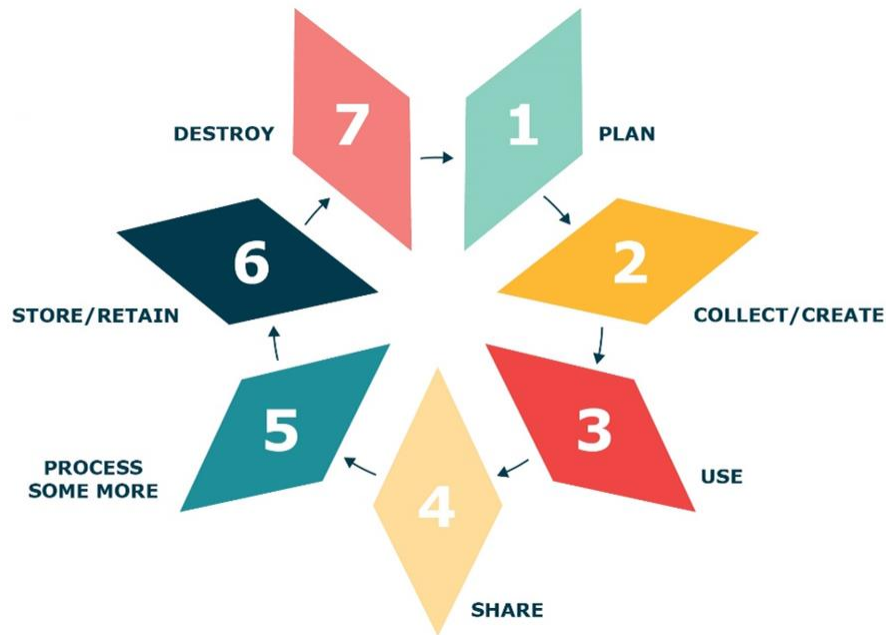
- collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or;
- merging, linking, as well as restriction, degradation, erasure or destruction of information.

²⁸ Future of Privacy Forum 'A visual guide to practical data de-identification', available at https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf

²⁹ Information classification is the process of assigning an appropriate level of classification to information to ensure that it receives an adequate level of protection. This definition is based on the concept governed by the International Organisation for Standardisation (ISO) ISO 27001 Information Security.

Processing activities are all part of the information lifecycle and POPIA applies to each phase of this information lifecycle.

Figure 1: The information lifecycle



2.1.2. Does the institution enter personal information into a record which forms part of a filing system?



Section 1 (Definition of records and filing system)
Section 3(4) (Definition of 'automated means')

For POPIA to apply, an institution must enter personal information into a [record](#) through using [automated](#) or non-automated means.

If the personal information is entered into a record by non-automated means, it must form part of or be intended to form part of a [filing system](#) to qualify as a record.

A record includes any form or medium, such as writing on any material, digital or computerised records, books, graphs, photographs, films, and tape recordings.

A filing system refers to a structured set of personal information 'which is accessible according to specific criteria', regardless of whether it is centralised or decentralised. This includes anything from a physical file in an alphabetised filing cabinet to multiple inter-related databases that can be accessed from anywhere in the world and that can handle complex search queries.

2.1.3. Is the institution domiciled in or is processing taking place in South Africa?

POPIA applies to all South African public universities because all public universities are domiciled in South Africa.

POPIA may also apply to institutions that are not domiciled in South Africa if another institution in South Africa is processing personal information on behalf of those institutions.

An institution is domiciled in South Africa if it is incorporated, established or formed in South Africa, or if it has its 'central management and control' in South Africa.³⁰

2.2. INSTITUTIONS MAY APPLY FOR AN EXEMPTION FROM POPIA



| Section 37 (Regulator may exempt processing of personal information)

A responsible party may apply to the Regulator for an exemption from the conditions for the lawful processing of personal information. An exemption could be a full exemption from all the conditions for the lawful processing of personal information or it could be granted for one or some of the conditions.

2.2.1. When institutions may apply for an exemption

Institutions may apply for an exemption to the Regulator for the processing of personal information. The Regulator may grant such an application after they considered the circumstances of the case and are satisfied that:

- the public interest in the processing substantially outweighs any interference with the privacy of the data subject that could result from the processing; or
- the processing involves a clear benefit to the data subject or a third party that substantially outweighs any interference with the privacy of the data subject or a third party that could result from the processing.

The Regulator may impose conditions in respect of any exemption granted. The conditions may include a requirement that the institution implement appropriate and reasonable technical and organisational measures to secure the integrity and confidentiality of the personal information.

2.2.1.1. When the processing is in the public interest

POPIA does not define public interest, however it provides examples where processing could be in the interest of the public, such as if processing takes place:

- for purposes of national security;

³⁰ The definition of 'resident' in terms of section 1 of the Income Tax Act 58 of 1962.

- to prevent, detect and prosecute offences;
- due to important economic and financial interests of a public body (e.g., a public body that intends to investigate fraud and corruption that impacts its economic and financial interests);
- to foster compliance with legal provisions established in the interests of the prevention, detection and prosecution of offences and important economic and financial interests of a public body;
- for historical, statistical and research purposes (refer to the Academy of Science of South Africa (Assaf) POPIA Compliance Standard); or
- due to the special importance of the interest in freedom of expression.

Public interest is the notion that an action, process or outcome widely and generally benefits the public at large and should be accepted, imposed or pursued for the sake of equality and justice. Public interest should not be limited in scope and application and the Regulator will assess it on a case-by-case basis.³¹

To apply for an exemption for the processing of personal information on the grounds of public interest, institutions must prove that:

- the specific processing activity is in the interest of the public; and
- the public interest is so significant that it outweighs the data subject's right to the protection of their personal information.

2.2.1.2. When the processing is to the clear benefit of the data subject

To apply for an exemption for the processing of personal information on the grounds of it being to the clear benefit of the data subject, institutions must:

- provide adequate reasons why the processing of personal information will be to the benefit of the data subject even though the processing would be in breach of the conditions for the lawful processing of personal information in POPIA;
- state the nature of the benefits to a data subject or third party; and
- specify how the benefit to a data subject or third party substantially outweighs any interference with the privacy of the data subject or third party.

³¹ The Information Regulator (South Africa) Guidance Note on exemptions from the conditions for lawful processing of personal information in terms of section 37 and 38 of the Protection of Personal Information Act 4 of 2013, 7, available at <https://infoeregulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-LawfulProcessing-202106.pdf>.

2.2.2. How institutions may apply for an exemption

Institutions must complete and submit the [Exemption Application Form](#) to the Regulator by email, post or hand delivery.³² If the Regulator grants an exemption, they will publish a notice in the Government Gazette. The exemption will come into force on the date of publication.³³

3. WHO IS RESPONSIBLE FOR POPIA COMPLIANCE

This section highlights how to identify responsible parties and operators and sets out the accountability of responsible parties.

3.1. HOW TO IDENTIFY RESPONSIBLE PARTIES AND OPERATORS



Section 8 (Responsible party to ensure conditions for lawful processing)
Section 1 definitions of responsible party and operator

The responsible party is the institution that has control over why and how personal information is processed; this includes deciding about:

- whether to collect personal information and the legal basis for collecting;
- which personal information to collect;
- what the personal information will be used for;
- whose personal information will be collected,
- whether to disclose the personal information, to whom, and under what circumstances;
- whether to give data subjects access to their personal information;
- how long to keep the personal information; or
- whether to make non-routine changes to personal information.

³² The Information Regulator (South Africa) Guidance Note on exemptions from the conditions for lawful processing of personal information in terms of section 37 and 38 of the Protection of Personal Information Act 4 of 2013, 11, available at <https://infoeregulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-LawfulProcessing-202106.pdf>.

³³ The Information Regulator (South Africa) Guidance Note on exemptions from the conditions for lawful processing of personal information in terms of section 37 and 38 of the Protection of Personal Information Act 4 of 2013, 14, available at <https://infoeregulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-LawfulProcessing-202106.pdf>.

When multiple institutions work together, there may be more than one responsible party taking part in a processing activity. Institutions may be jointly responsible if they take joint decisions about the purposes and means of processing personal information.

Responsible parties are also responsible for the actions of their employees, provided that the actions of the employees are within the course and scope of their employment.³⁴

Sometimes organisations process personal information even though they have no control over why and how that personal information is processed. These organisations are most likely operators.

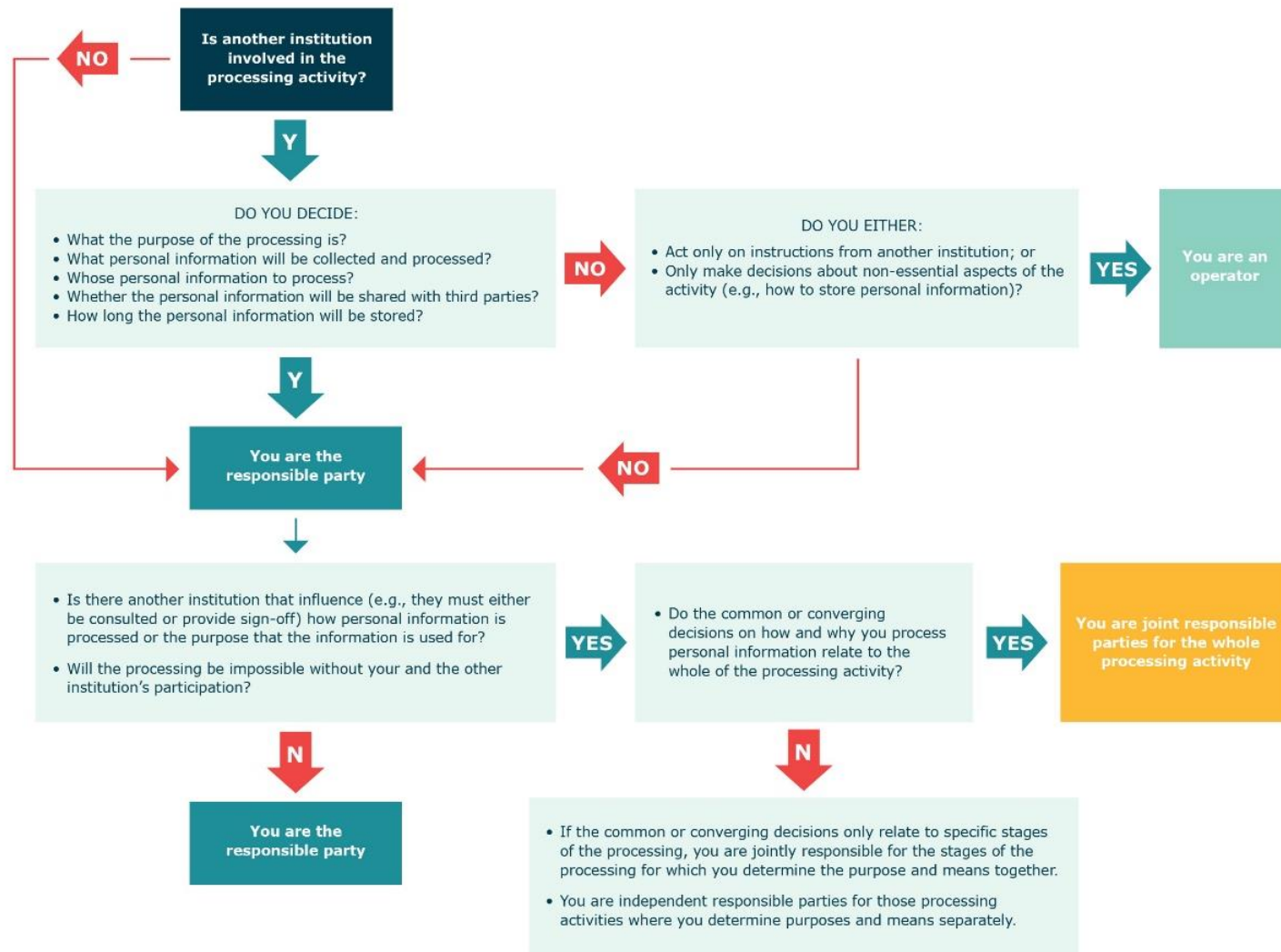


An [operator](#) is a person who processes personal information for a responsible party in terms of a contract or mandate without coming under the direct authority of the responsible party.

The following flowchart shows the questions institutions must answer to identify responsible parties and [operators](#).

³⁴ *K v Minister of Safety and Security* 2005 (6) SA 419 (CC) paragraph 24.

Figure 2: Questions institutions must answer to identify responsible parties and operators





Here are some common examples:

Example: A public university provides teaching and learning services to students. To provide these services, the university must collect the names, identity numbers, contact details and previous education of the students. This university is the responsible party.

Example: A university appoints a law firm to represent them in a dispute about unpaid student fees. To do this, the law firm must process personal information relating to the dispute. The reason for processing the personal information is the law firm's mandate to represent the institution in court. This mandate, however, is not specifically targeted to personal information processing. The law firm decides what information to use and how to use it to recover unpaid student fees. The university does not provide the law firm with any specific instructions on how to process the personal information. In this example, the law firm acts with a significant degree of independence, such as deciding what personal information to collect and what to use it for. The law firm's processing activities to fulfil the task as legal representative for the institution are therefore linked to the functional role of the law firm, which means that it is the responsible party for this processing activity.³⁵

Example: A university uses a learning management system provided by LMS (Pty) Ltd. Students' names, email addresses, student numbers and test results are stored by LMS (Pty) Ltd. LMS (Pty) Ltd is the operator, and the university is the responsible party.

Example: Several universities decide to take part in a joint research project. One of the universities has a state-of-the-art research management platform. The universities decide to make use of this platform to store the research data they collect. The universities are jointly responsible, because they determined the purpose for the processing and decided together to store and disclose personal information on this particular platform. Refer to the Assaf POPIA Code of Conduct for more about determining accountability in research projects.

Example: A university asks a recruitment agency to help them find a suitable candidate for a vacancy. The recruitment agency searches its own extensive database of CVs and the CVs received from the university. The university agrees that the CVs which they submitted to the recruitment agency may be included in the agency's database. The university and the recruitment agency are jointly responsible because they jointly participate in the processing activity with the purpose of finding suitable candidates.

3.2. ACCOUNTABILITY OF RESPONSIBLE PARTIES



Section 8 (Responsible party to ensure conditions for lawful processing)

Section 55 (Duties and responsibilities of Information Officers)

Regulation 4 (Responsibilities of Information Officers)

Responsible parties must ensure that they meet the conditions for the lawful processing of personal information. When institutions process personal information with other organisations, they must:

³⁵ The European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR p12. Available at https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

- identify responsible party(s) and operators involved in the activity;
- ensure that there is no confusion about their respective roles and responsibilities for POPIA compliance;
- establish their roles and responsibilities before the processing of personal information starts;
- document their roles and responsibilities in a written agreement;
- conclude agreements with operators in which they agree:
 - to only use personal information when they have the responsible party's written authority;
 - that the personal information is confidential and that they must not share it with third parties without the responsible party's written authority;
 - to implement appropriate safeguards when processing personal information;
 - to notify the responsible party as soon as reasonably possible if there was a security compromise; and
 - to take any additional steps the responsible party requires to comply with POPIA; and
- comply with the transborder information flow requirements where personal information is transferred to a third party in another country.

All institutions must appoint an Information Officer, and, if the institution is large enough, also Deputy Information Officers. Institutions must register Information Officers and Deputy Information Officers with the Regulator.³⁶

POPIA sets out various duties and responsibilities of Information Officers. In terms of POPIA Information Officers must:

- create a POPIA compliance framework;³⁷
- encourage that the institution comply with the conditions for the lawful processing of personal information;³⁸

³⁶ See the [Information Regulator's Guidance Note on Information Officers and Deputy Information Officers](#) for further guidance.

³⁷ POPIA Regulation 4(a).

³⁸ Section 55(1)(a).

- create, publish, and implement a Promotion of Access to Information Act (PAIA) Manual;³⁹
- complete and document a Personal Information Impact Assessment (PIIA) on its processing activities;⁴⁰
- ensure that all staff involved in personal information processing activities receive training on their data protection responsibilities;⁴¹
- deal with requests made to the institution in terms of POPIA;⁴² and
- work with the Regulator on investigations conducted in relation to the institution.⁴³

4. HOW TO ASSESS COMPLIANCE

This section explains how responsible parties must assess if they are POPIA compliant through establishing if they have to do a PIIA and how to do it. This is followed by a discussion of POPIA's conditions for the lawful processing of personal, special personal and children's personal information. Lastly this section discusses the rights of the data subjects concerning the processing of their personal information.

4.1. RESPONSIBLE PARTIES MUST ASSESS POPIA COMPLIANCE



Section 8 (Responsible party to ensure conditions for lawful processing)
Regulation 4 (Responsibilities of Information Officers)

Responsible parties are accountable to ensure that they comply with POPIA. As POPIA applies to all processing activities, responsible parties must complete and document a PIIA on their processing activities. Processing activities include any activities where personal information is being processed, whether it is collected, used, stored or destroyed.

4.1.1. How an institution must do a PIIA

A PIIA must at least include the following:

- a description of the envisaged processing activity and the purpose of the processing;⁴⁴

³⁹ POPIA Regulation 4(c).

⁴⁰ POPIA Regulation 4(b).

⁴¹ POPIA Regulations 4(e).

⁴² Section 55(1)(b).

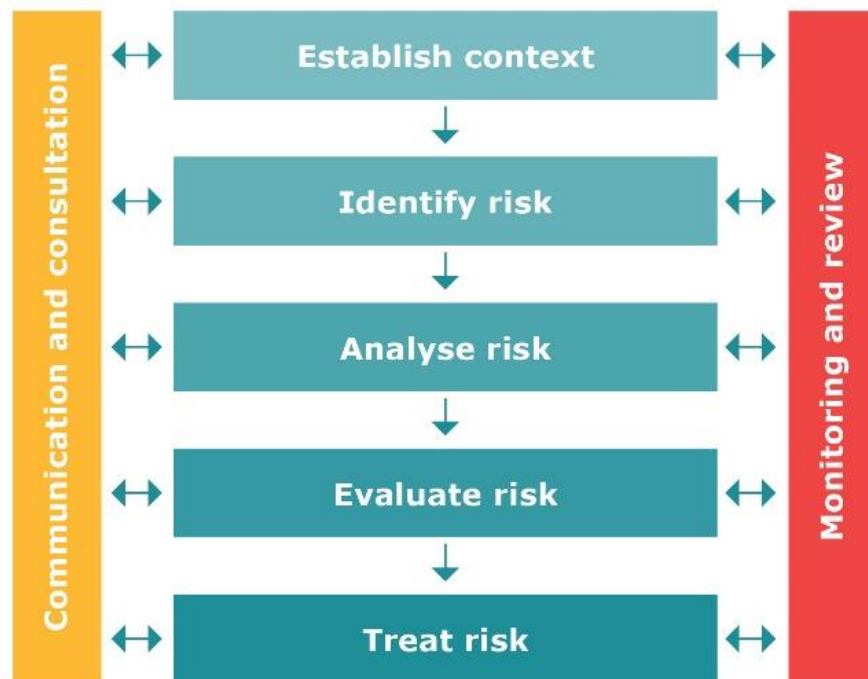
⁴³ Section 55(1)(c).

⁴⁴ Recital 90 of the GDPR.

- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects (this includes the 'origin, nature, particularity and severity of that risk');⁴⁵ and
- the measures envisaged to address the risks and demonstrate compliance.

Assessing, analysing and evaluating risk is an integral part of POPIA compliance. This is often referred to as a risk management process and is illustrated in the following image.

Figure 3: Risk management process



Here is a brief explanation of what each of these phrases means:

Communication and consultation: Effective risk management relies on effective communication and consultation. Stakeholders will make decisions based on how they perceive certain risks, and ineffective

⁴⁵ Recital 84 of the GDPR.

or incomplete communication can undermine these decisions. Also, informed stakeholders can help identify risks.

Establish the context: Before the institution can identify risk, it must understand the context in which it operates. The institution should ask what the internal and external circumstances or conditions are that could keep it from achieving its goals. The institution must consider the conditions in the country and in higher education, but also the context of the specific institution when doing this exercise.

Identify the risk: The institution must identify risks and lost opportunities by taking various approaches (quantitative, qualitative, or semi-qualitative) and by using different tools (risk registers, competitor analysis, market trend research, SWOT analyses, internal questionnaires).

Analyse the risk: Once the institution has identified its risks, it should try to understand those risks by analysing their causes and sources, and gathering the information it needs to evaluate those risks. The institution can assess its existing controls, analyse the consequence and likelihood of a risk and estimate the probability thereof. The institutions can also monitor risk probability, obtain expert opinions, complete risk registers, and account for uncertainties.

Evaluate the risk: After analysing a risk, the institution should measure each risk against pre-determined criteria to establish how significant that risk is and to assign a rating to the risk. This is when the institution should rate how likely and probable the risk is, what the impact or severity of that risk could be, and if its existing controls are adequate in addressing the risk. At this stage, the institution may immediately accept some risks 'as is' or take steps to avoid the risk.

Treat the risk: Next, the institution must decide what to do about the risks it has identified. Generally, it must choose to either accept or tolerate the risk, avoid the risk, remove the source of the risk, change the likelihood and the consequences of the risk, transfer the risk, or exploit the opportunity. While considering how to manage the risk, the institution should develop and implement a risk response plan.

Monitor and review: Finally, the institution should monitor and review risk continuously to help ensure that risk management works. The institution must plan, examine and evaluate risk and it must record the results of the process and communicate those results so as to improve the risk management process.

This methodology could also be applied to opportunities that might have been missed, such as creating a new process, product or service, or improving existing processes, products or services, or improving the reputation of, and trust in the institution, or building or strengthening relationships with new and existing stakeholders.



Recommendation:

Follow the eight steps to do a PIIA in paragraph 6.8.

4.1.2. When an institution must do a PIIA

POPIA does not indicate when institutions should perform a PIIA. It is up to the institution to decide when it must complete a PIIA. Institutions can use PIIAs to assess their POPIA compliance risk, to bring their existing processes, products or services in line with POPIA requirements and to assess compliance with internal data protection policies.

Institutions can also use PIIAs to measure the impact of a change in a processing activity to ensure that the change has not introduced new compliance risks.

Institutions should do a PIIA when they:

- process personal information for a new purpose;
- launch new products or services;
- expand into other countries;
- introduce new systems, software or hardware for processing;
- share personal information with third parties; or
- use a new service provider or supplier.

Institutions must also update their past PIAs if POPIA is amended, new regulations are passed, if the Regulator publishes new guidance notes and with the development of new caselaw.

4.2. INSTITUTIONS MUST RECORD THEIR PROCESSING ACTIVITIES



Section 17 (Documentation)

POPIA requires that institutions must document all their processing activities. In addition, institutions must store information about their processing activities to be able to respond to requests from data subjects and the Regulator.



Recommendation:

Institutions should keep a record of processing activities (ROPA).⁴⁶

Institutions must publish a PAIA manual describing, amongst other things:⁴⁷

- the purpose of processing personal information;
- the categories of data subjects and the categories of personal information;
- the recipients or categories of recipients to whom the personal information may have been supplied;
- the planned transborder flows of personal information; and

⁴⁶ See the UK Information Commissioner's Office's guidelines on documenting processing activities for examples, guidance and templates, available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/documentation/>

⁴⁷ Section 14 of PAIA. Refer to the template published by the Regulator at <https://info regulator.org.za/wp-content/uploads/2020/07/PAIA-Manual-Template-Public-Body.pdf>

- in general, the information security measures they implemented.

4.3. INSTITUTIONS MUST DETERMINE AND DOCUMENT THE PURPOSE FOR PROCESSING PERSONAL INFORMATION



| Section 13(1) (Collection for specific purpose)

Institutions must document a specific, explicitly defined, and lawful purpose for collecting personal information. Before collecting personal information, institutions must know the lawful purpose of each piece of personal information they collect. To say that "we might need this personal information in future" does not constitute a lawful purpose to collect that personal information.



Example: Institutions collect and process students' personal information to provide teaching and learning services, support services, accommodation, medical services and sporting facilities to them.

Example: Institutions are required by law, such as the Higher Education Act, Health Professions Act, National Qualifications Framework Act and Engineering Professions Act, to collect and, in some cases, share students' personal information.

Example: Institutions collect, use and create personal information of employees to manage employment relationships, such as to pay salaries, deduct tax, manage leave, provide training, handle disciplinary proceedings and ensure the health and safety of employees.

Example: Institutions collect qualifying donor's personal information to issue tax certificates.

4.4. INSTITUTIONS MUST KEEP PROCESSING TO A MINIMUM



| Section 10 (Minimality)

The principle of minimality states that personal information may only be processed if it is adequate, relevant and not excessive for the purpose for which it is processed. When an institution plans a processing activity, the institution must document the purpose for processing and the pieces of personal information that are absolutely required to achieve that purpose. If the institution does not have access to adequate and relevant information, the processing activity will not achieve its purpose, however, institutions must also not collect excessive information to achieve their purpose – only the absolute necessary information may be collected lawfully.

4.4.1. Personal information must be adequate

Information is adequate if it is of acceptable quality or quantity – information will be inadequate if it is incomplete, out of date, or inaccurate.

4.4.2. Personal information must be relevant

Institutions may only collect personal information that is relevant and appropriately connected to the purpose of processing. If the personal information is not needed to achieve the purpose, the institution does not have the right to retain the information because it is not relevant.



Example: The fact that a person was declared insolvent 15 years ago, is no longer relevant when an institution wants to assess the person's ability to work with money.⁴⁸

Example: An IT support centre records the telephone conversations between support staff and students for training purposes. The full telephone conversations, including students' contact information and passwords, are stored permanently for this purpose. The person in charge of support staff training listens to only one recording per staff member per week. Keeping full and permanent recordings of all support calls is excessive for employee training purposes and also introduces a huge security risk which should not be allowed.⁴⁹

4.4.3. Personal information must not be excessive

Institutions must not collect more personal information than what is absolutely needed to fulfil the purpose for which the information is being collected. Collecting personal information just in case it may be used in future is unacceptable. However, institutions may collect personal information needed for a foreseeable event that may occur.



Example: An institution may collect information about students' health (e.g., asthma and type 1 diabetes) when providing student accommodation as this information is necessary in case of a medical emergency, even though an emergency may never occur.

4.5. INSTITUTIONS MUST HAVE A LEGAL BASIS FOR PROCESSING



Section 4 (Lawful processing of personal information)
 Section 9 (Lawfulness of processing)
 Section 11 (Consent, justification and objection)
 Section 26 (Prohibition on processing of special personal information)
 Section 27 (General authorisation concerning special personal information)
 Section 34 (Prohibition on processing personal information of children)
 Section 35 (General authorisation concerning personal information of children)

POPIA provides a closed list of legal justifications for processing personal information. At least one of them must apply for a processing activity to be legal. However, complying with these legal justifications is difficult as different justifications apply to different classes of personal information. That is why it is important that an institution must be clear about the purpose for processing personal information and

⁴⁸ This is referred to as the 'right to be forgotten'. See *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Marion Costeja Gonzalez* C-131/12. The decision was based on articles 2, 4, 12 and 14 of 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 which deal with the national laws applicable, a data subject's right of access and a data subject's right to object respectively. This right is expressly included in article 17 of the GDPR. It has not been expressly included in POPIA, but, based on the Google Spain decision and the fact that section 10 is so similar to article 17 of the Data Protection Directive of 1995, a similar interpretation will likely be followed in South Africa.

⁴⁹ CNIL adopts its first sanction as lead supervisory authority, fining French online shoe retailer (11 August 2020) available at: <https://www.natlawreview.com/article/cnil-adopts-its-first-sanction-lead-supervisory-authority-fining-french-online-shoe>.

must have identified the relevant personal information required to achieve that purpose before determining the legal justification for each piece of personal information.

The justifications for processing [special personal information](#) and the personal information of [children](#) are stricter than for other classes of personal information.

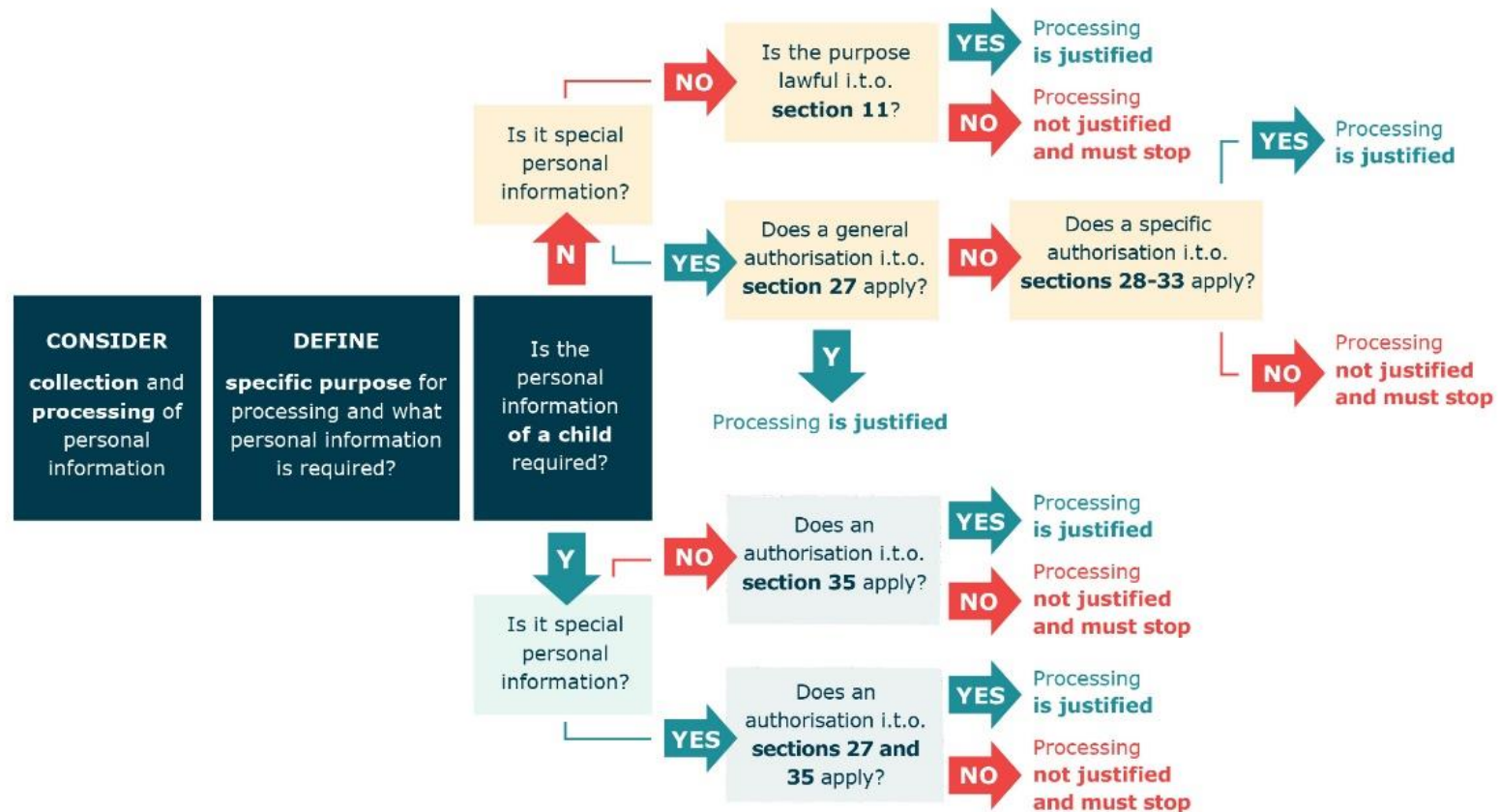


Special personal information is information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. It is also information concerning the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence, or any proceedings in respect of any offence that the data subject allegedly committed or the disposal of such proceedings.

Child means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

In the following diagram, a process is set out for institutions to determine the appropriate legal justification required for each piece of personal information:

Figure 4: Appropriate legal justification for each piece of personal information



4.5.1. When institutions may process personal information



Section 11 (Consent, justification and objection)

If personal information is not special personal information or the personal information of children, then there are six justifications for processing personal information. Institutions can process personal information if the:

- processing is necessary to carry out actions to conclude or perform in terms of a contract;
- processing complies with a legal obligation imposed on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body;
- processing is necessary to pursue the legitimate interests of the responsible party or of a third party to whom the information is supplied; or
- data subject consents to processing.

4.5.1.1. Personal information may be processed to conclude or perform in terms of a contract

If personal information is 'necessary' for the institution to conclude a contract or to perform in terms of a contract with the data subject, the processing of that personal information is justified.

The word 'necessary' must be interpreted narrowly. The institution must be able to justify the necessity of the processing activity with regards to the fundamental and mutually understood purpose of the contract.

Institutions can rely on this justification if:	Institutions cannot rely on this justification:
• they have a contract with a data subject and they need to process the data subject's personal information to comply with their responsibilities in terms of that contract; • they have a contract with a data subject and they need to process the data subject's personal information so that they can comply with any counter-obligations in the contract; or • they don't have a contract with the data subject yet, but the data subject asked them to take a step towards an agreement and the institution must	to process special personal information or the personal information of children.

process the data subject's personal information to take that step.⁵⁰



Example: Student application

When prospective students apply to a public university, they are asked to provide personal information for the university to apply its admissions policy. It is necessary to process this personal information to consider the student's application and to eventually conclude a contract with the student if the application was successful. Similarly, when a student applies for funds or a loan it is necessary to collect the personal information of the applicant to do a means test. These processing activities are clearly necessary for the institution to enter into a student contract or a funding or loan agreement with the student. However, this justification does not extend to creating a profile of the student's lifestyle choices even if profiling is mentioned in the contract. This is because the institution has not been contracted to perform profiling. The institution must then rely on another justification for such a processing activity.

Example: Employment contract

Many processing activities that involve the personal information of employees are justified because they are necessary to conclude an employment contract with the employee and for the institution to perform in terms of that contract, for instance, when the institution must process bank account details of its employees to pay salaries. However, this will not be the case for all processing activities. For example, electronic monitoring of employees' use of the internet or telephones and video surveillance often goes beyond what is necessary for the performance of the employment contract. The institution should rely on the justification that it is in its legitimate interest to monitor employees.

Example: Online services

When a data subject must accept online terms and conditions in order to access a service, the institution may rely on that digital contract to process personal information which is necessary to provide services. However, the digital contract cannot be used as a basis for the institution to advertise and market its other services as such marketing is not necessary to perform in terms of the contract. To advertise and market its other services, the institution must establish and rely on a different justification, such as its legitimate interest or the consent of the data subject.

4.5.1.2. Personal information may be processed to comply with a legal obligation

If the law requires that a particular processing activity must take place, the processing is justified, such as when the Government is legally authorised to collect personal information.

Institutions can rely on this justification if:	Institutions cannot rely on this justification:
it has a legal obligation to process personal information in terms of the Constitution, common law, customary law, legislation or court decisions.	if the legal provision itself is not POPIA compliant;⁵¹ or to process special personal information or the personal information of children.

⁵⁰ The ICO's guidance and resources to the UK GDPR, available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/contract/>

⁵¹ Section 3(2)(a). For instance, the processing prescribed must be necessary to fulfil the purpose of the legal provision and it must be the least invasive way to achieve that purpose.

**Recommendation:**

If there are contradictory legislative requirements the institution may refer any contradictory legislative requirements to USAf, who will refer the matter to the POPIA Forum to consider appropriate action.

**Example: Complying with reporting requirements**

Some student information is collected in order to comply with the reporting requirements placed on public universities by the Department of Higher Education and Training in terms of the Higher Education Act.

Example: Labour legislation

The Employment Equity Act, the Labour Relations Act, and the Basic Conditions of Employment Act provide justification for the processing of many categories of employee information.

4.5.1.3. Personal information may be processed to protect a legitimate interest of the data subject

If the processing of personal information protects the legitimate interests of the data subject, it will be lawful. A legitimate interest of a data subject includes vital interests such as safety, health, humanitarian purposes, emergencies, and other interests such as financial interests.

Institutions can rely on this justification:	Institutions cannot rely on this justification:
• for unusual processing activities involving small numbers of records that benefit the data subject; • in an emergency or a dangerous situation; • on humanitarian grounds; or • to prevent harm to a data subject.	• for large-scale, planned processing activities; or • to process special personal information or the personal information of children.

When an institution relies on the legitimate interest justification, data subjects can object to the processing activity at any time 'on reasonable grounds relating to his, her or its particular situation'.⁵² Data subjects must be notified of their right to object.⁵³ If the data subject's objection is valid, the institution may no longer process the data subject's personal information.⁵⁴

⁵² Section 11(3)(a). This data subject right is discussed in paragraph 4.13.5.

⁵³ Section 18(1)(h)(iv).

⁵⁴ Section 11(4).

**Example: Student threatens self-harm**

A student threatens self-harm in a social media post. The institution would be justified in disclosing the student's personal information to the authorities to intervene.

Example: Receiving appropriate support from the institution

It is in a student's legitimate interest for the university to learn about its students to intervene and provide effective support to the student.

4.5.1.4. **Personal information may be processed by a public body to ensure proper performance of a public law duty**

If processing of personal information is necessary for a public body to perform a public law duty, that processing activity will be justified. The word 'necessary' must be interpreted narrowly. Whether the particular processing activity is necessary must be measured against the exact reason for the public function, in other words, the institution must consider the substance and fundamental objective of the public function.

**Public body means:**

- any department of state or administration in the national or provincial spheres of government or any municipality in the local spheres of government; or
- any other functionary or institution when:
 - exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
 - exercising a public power or performing a public function in terms of any legislation.

Public universities can rely on this justification:	Public universities cannot rely on this justification:
when the institution is a public body performing a public function in terms of any legislation. ⁵⁵	to process special personal information or the personal information of children.

When an institution relies on this justification, data subjects can object to the processing activity at any time 'on reasonable grounds relating to his, her or its particular situation'.⁵⁶ Data subjects must be notified of their right to object.⁵⁷ If the data subject's objection is valid, the institution may no longer process the data subject's personal information.⁵⁸

⁵⁵ A public university is an 'organ of state' as defined by the Constitution of South Africa.

⁵⁶ Section 11(3)(a). This data subject right is discussed in paragraph 4.13.5.

⁵⁷ Section 18(1)(h)(iv).

⁵⁸ Section 11(4).



Example: Submitting information to the Department of Higher Education and Training

The Department of Higher Education and Training requires information from public universities to fulfil its mandate.

4.5.1.5. Personal information may be processed to ensure the legitimate interest of the responsible party or of a third party

Processing personal information is justified if the activity is necessary to pursue the legitimate interests of the responsible party, or that of a third party to whom the information is supplied. The responsible party's interest in the processing must be distinguished from the purpose of the processing activity. The purpose is the specific reason why the personal information is processed, whereas the responsible party's interest in the processing activity is the broader stake that it has in the processing or the benefit that it might derive from the processing activity.

The legitimate interest of the responsible party or third party must be weighed against the rights and interests of the data subject to ensure that there is no disproportionate infringement of privacy. The responsible party or third party must show that the limitation of the data subject's right to privacy is reasonable.⁵⁹



Recommendation:

For institutions to rely on this justification they must perform a **legitimate interest assessment (LIA)** consisting of three steps. Institutions must:⁶⁰

1. Identify the legitimate interests of the institution or third party by asking these questions:
 - What is the purpose for processing the personal information?
 - Who benefits from the processing?
 - In what way does the institution or third party benefit from the processing?
 - Is the interest a fundamental right (e.g., freedom of expression or the right of access to information)?
 - Is there a wider public benefit to the processing?
 - How important is the wider public benefit of the processing?
 - What would be the impact if processing cannot go ahead?
 - Does the law or society recognise the interest?

⁵⁹ Section 36 of the Constitution of South Africa.

⁶⁰ UK ICO Guidance and Resources on the UK GDPR available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/>

2. Apply the necessity test by asking these questions:
 - Does the processing actually help furthering the responsible party or third party's interest?
 - Is the proposed processing a reasonable way to achieve the purpose?
 - Is there another less intrusive way to achieve the same result?
3. Perform a balancing test by considering the impact of the processing on the data subject's right to privacy and whether this overrides the identified interests by asking these questions:
 - What is the nature of the relationship between the institution or third party and the data subject?
 - Is any of the information particularly sensitive or private?
 - Would data subjects expect the institution to use their information in this way?
 - How easily can the institution explain the processing of personal information to a data subject?
 - Are some data subjects likely to find the processing objectionable or intrusive?
 - How big an impact might the processing have on data subjects?
 - Are any data subjects particularly vulnerable (e.g., previously disadvantaged)?
 - What safeguards are in place to minimise the impact on data subjects?

To minimise the impact that processing might have on data subjects it is recommended that:

- there are strict limitations on how much personal information is collected;
- the personal information is immediately limited after its use;
- there are technical and organisational measures in place to keep the personal information secure;
- personal information must be anonymised; and
- there is increased transparency.

Institutions can rely on this justification if:	Institutions cannot rely on this justification:
the impact on the data subject is insignificant or the legitimate interest of the responsible party or third party overrides the impact on the data subject's right to privacy.	to process special personal information or the personal information of children.

When an institution relies on their or a third party's legitimate interests, data subjects can object to the processing activity at any time 'on reasonable grounds relating to his, her or its particular situation'.⁶¹ Data subjects must be notified of their right to object.⁶² If the data subject's objection is valid, the institution may no longer process the data subject's personal information.⁶³



Examples of when institutions may rely on the legitimate interests of the responsible party or a third party to process personal information would be:

- When it is in the institution's economic interest to learn as much as possible about its students so that it can effectively intervene before a student fails.
- When the institution has processing activities that are related to performing in terms of a contract or to comply with legislation that are strictly speaking not 'necessary'.
- When the institution must enforce legal claims such as debt collection.
- If the institution tries to prevent fraud or the misuse of services.
- If the institution must process personal information for historical, scientific, or statistical purposes.
- When the institution monitors its employees for safety or management purposes.
- When the institution does fundraising.
- When processing personal information forms part of a whistleblowing scheme.
- When processing is done for research purposes.⁶⁴
- If the institution is doing non-electronic direct marketing and advertising.⁶⁵

⁶¹ Section 11(3)(a). This data subject right is discussed in paragraph 4.13.5.

⁶² Section 18(1)(h)(iv).

⁶³ Section 11(4).

⁶⁴ Refer to the Assaf POPIA compliance standard for more on how POPIA applies to research activities.

⁶⁵ 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 25. Direct marketing is discussed in paragraph 5.2.

4.5.1.6. Personal information may be processed with the consent of the data subject

If the data subject consents to the processing of their personal information, then the processing is justified.



Consent means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

Consent will thus be valid if it is voluntary, specific, informed and an expression of will – and only if all of these elements are present.

This is what these elements mean in practice:

Voluntary	Consent must be the genuine choice of the data subject. This means that the data subject must be able to say no, but still continue with the activity (e.g., apply to study at the institution). Consent must not be tied to some performance in terms of a contract. The contract must be able to continue without the processing of personal information for which consent is required.⁶⁶ Data subjects must be free to easily withdraw their consent and without any detrimental effects such as an increase in cost, a cessation of services or a decrease in service levels.⁶⁷ Example: Voluntary consent A student applies to study at a university. During the application process the university asks them to submit a photograph that the university can use in direct marketing to prospective students. Submitting a photograph for direct marketing is not a requirement for the university to provide their teaching and learning services to the applicant. The applicant can choose not to provide a photograph and continue with their application. Withholding consent does not affect their application, and the contract can continue without the applicant's consent.
Specific	The consent must always relate to a specific, well-articulated purpose. A blanket consent covering all purposes for which personal information is processed will be too vague to be valid. Instead, consents must be highly detailed.⁶⁸
Informed	Institutions must provide specific information with each consent request to inform the data subject of the choices they have.⁶⁹ When asking the data subject for consent, the institution must provide:⁷⁰ • the institution's identity;

⁶⁶ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 10.

⁶⁷ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 24.

⁶⁸ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 14.

⁶⁹ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 14.

⁷⁰ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 15.

	• the purpose for each of the processing activities for which the consent is sought; • the type of personal information that will be collected and used; • whether the information will be used for automated decision-making; and • that the data subject has the right to withdraw consent at any time.
Expression of will	The data subject's consent must be explicit, which means that it must be given by means of a clear, unambiguous, affirmative act. It cannot be given by default or silence, nor can inactivity be taken as consent. The action of giving consent must be distinct from other actions such as agreeing to terms and conditions. ⁷¹

Data subjects have the absolute right to withdraw consent.



Recommendation:

Managing consents obtained and withdrawn can be very tricky. Institutions should have an easy-to-use central consent management system that is available to everyone who may need to rely on a consent.



Example: Consent to use personal information to improve services

When registering for an e-learning platform, a student is asked to consent to the use of their identifiable information to improve the course content. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, 'I consent', the student gives voluntary, specific and informed consent to the institution.

Example: Employees consent to be filmed

A film crew is going to be filming a certain part of an office. The institution asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.⁷²

⁷¹ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 18.

⁷² European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 9.

4.5.2. When institutions may process special personal information



Section 26 (Prohibition on processing of special personal information)

Section 27 (General authorisations concerning special personal information)

The default position is that institutions are prohibited from processing [special personal information](#). However, POPIA provides a list of general authorisations for the processing of special personal information and additional specific authorisations specific to the type of special personal information. In other words, to process special personal information, an institution must either have a general authorisation or a specific authorisation for the type of special personal information being processed.

For institutions to establish when they may process special personal information they must:

- identify the activities where they plan to process or are already processing special personal information; and
- determine and document which general or specific authorisation they rely on per piece of special personal information.

In terms of POPIA there are general authorisations in terms of the processing of special personal information. When one of these general authorisations exist, institutions may process special personal information. The general authorisations are:

- Data subjects have consented to processing.
- Processing is necessary for the establishment, exercise or defence of a right or legal obligation.
- Processing is necessary to comply with an obligation of international public law.
- Processing is for historical, statistical or research purposes.
- The data subject deliberately made the special personal information public.
- The Information Regulator has authorised the processing of special personal information.
- Processing is necessary for a medical institution to provide proper treatment or care.

Processing is necessary to supplement criminal behaviour or biometric information.

4.5.2.1. Data subjects have consented to processing

The requirements discussed in paragraph 4.5.1.6 applies.

4.5.2.2. Processing is necessary for the establishment, exercise or defence of a right or legal obligation

This authorisation allows institutions to process special personal information where it is necessary to exercise a right or claim it has in terms of South African law, such as a right to access to information, a claim for money owed, property rights and contractual claims.

4.5.2.3. Processing is necessary to comply with an obligation of international public law

Public international law has three main sources, namely customary international law, treaties, and conventions. Section 39 of the South African Constitution requires that, when interpreting the Bill of Rights, courts or other legal bodies must consider public international law. The South African Constitution furthermore recognises international customary law as law in South Africa unless it is inconsistent with the Constitution or local legislation.⁷³ In addition, once an international treaty or convention has been approved by the National Assembly and the National Council of Provinces, South Africa is bound by them.⁷⁴

4.5.2.4. Processing is for historical, statistical or research purposes

Historical purposes include archiving and processing personal information of or concerning history or past events. In most cases, institutions will be required to process personal information for historical purposes by the National Archives and Record Services of South Africa Act,⁷⁵ in which case the institution will be authorised to process the information due to an obligation in law as discussed in paragraph 4.5.2.2.

Statistical purposes cover a wide range of processing activities, from commercial purposes to public interest.⁷⁶ It refers to any operation of collecting and processing information necessary for statistical surveys or for the production of statistical results.⁷⁷

Research purposes include the activities that are aimed at improving knowledge of any discipline through enquiry or systematic investigation, such as academic research, scientific research, commercial or industrial research, and technological development and demonstration.

To rely on this authorisation institutions must provide **sufficient guarantees** that the individual privacy of the data subject is not adversely affected, AND that EITHER processing is necessary to serve a [public interest](#); OR that to ask for consent appears to be impossible or would involve disproportionate effort (virtually impossible).

The **sufficient guarantees** that an institution must provide that the individual privacy of the data subject would not adversely be affected may include:

⁷³ Section 232 of the Constitution of the Republic of South Africa, 1996.

⁷⁴ Section 231 of the Constitution.

⁷⁵ Act 43 of 1996.

⁷⁶ Article 29 Data Protection working Party *Opinion 03/2013 on purpose limitation* 29.

⁷⁷ Recital 162 of the European Union General Data Protection Regulation 2016/679.

- having strict limitations on how much personal information is collected;
- immediately deleting the personal information that is not used;
- applying technical and organisational measures to keep personal information secure;
- anonymising the personal information;
- increasing transparency;
- providing an easy-to-use opt-out; and
- complying with an applicable issued code of conduct.

4.5.2.5. The data subject deliberately made the special personal information public

An institution may process special personal information if the information was deliberately made public by the data subject.

The institution must be able to determine that the data subject intended to publish their special personal information to the public without impediment or protective mechanism that prohibits the public from having access to the information.

4.5.2.6. The Information Regulator has authorised the processing of special personal information

An institution may apply to the Regulator for authorisation to process special personal information and the Regulator may authorise the processing of special personal information by notice in the Government Gazette if:⁷⁸

- the processing was in the [public interest](#); AND
- appropriate safeguards have been put in place to protect the special personal information such as the technical and organisational security measures discussed in paragraph 4.9.⁷⁹

⁷⁸ Information Regulator South Africa Guidance Note on Processing of Special Personal Information 6.

⁷⁹ Information Regulator South Africa Guidance Note on Processing of Special Personal Information 7.

4.5.2.7. Processing is necessary for a medical institution to provide proper treatment or care



Section 32(4) (Authorisation concerning data subject's health and sex life)

Medical institutions may supplement information about a data subject's health with other types of special personal information, to provide proper treatment or care.⁸⁰



Example: Confirming a person's religious beliefs may be necessary before providing treatment

Medical practitioners may need to confirm that a person's religious beliefs allow them to receive a blood transfusion or heart transplant.

4.5.2.8. Processing is necessary to supplement criminal behaviour or biometric information



Section 33(3) (Authorisation concerning a data subject's criminal behaviour or biometric information)

It may be necessary to supplement information about a data subject's criminal behaviour or biometric information if the processing is carried out by institutions charged by law with applying criminal law or by responsible parties who have obtained that information legally.⁸¹



Example: It may be necessary to supplement biometric information with information about a person's health for research purposes.

4.5.3. Specific authorisations for processing religious or philosophical beliefs



Section 28 (Authorisation concerning data subject's religious or philosophical beliefs)

Personal information concerning religious or philosophical beliefs may be processed:

- by spiritual or religious institutions of their members or if the activity is necessary to achieve the aims and principles of the organisation;

⁸⁰ Even though this authorisation is listed with the specific authorisations concerning a data subject's health or sex life, we list it here because it is an authorisation for processing all other types of special personal information.

⁸¹ Even though this authorisation is listed with the specific authorisations concerning a data subject's criminal behaviour or biometric information, we list it here because it is an authorisation for processing all other types of special personal information.

- by spiritual or religious institutions of family members of their members if the organisation maintains regular contact with them in connection with its aim and the family members have not objected in writing;
- by institutions founded on religious or philosophical principles of their members, employees, or other data subjects if it is necessary to achieve their aims and principles; and
- by other institutions if the processing is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.



Example: Halaal and Kosher meals

An institution may want to know whether students need Halaal or Kosher meals in order to meet their needs.

4.5.4. Specific authorisations for processing race or ethnic origin



| Section 29 (Authorisation concerning a data subject's race or ethnic origin)

Processing information relating to race or ethnic origin is authorised if:

- the processing is essential to identify the data subject; AND
- the processing is required to comply with legislation and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.



Example: Race information required by legislation

Institutions may process information relating to race or ethnic origin to comply with the Broad-based Black Economic Empowerment Act 53 of 2003, B-BBEE Codes of Good Practice as well as the Employment Equity Act 55 of 1998.

4.5.5. Specific authorisations for processing trade union membership



| Section 30 (Authorisation concerning data subject's trade union membership)

A trade union (or the trade union federation to which the trade union belongs) may process the trade union membership of its own members if the processing is necessary to achieve the aims of that trade union (or the trade union federation). The trade union or trade union federation is not permitted to share this personal information with third parties without the data subject's consent, unless one of the other general authorisations apply to the sharing activity.

4.5.6. Specific authorisations for processing political persuasion



| Section 31 (Authorisation concerning data subject's political persuasion)

Political institutions are not allowed to share personal information with third parties without the consent of the data subject, unless one of the general authorisations apply. This means that an institution founded on political principles may process information relating to the political persuasion of data subjects if:

- the data subjects are members of the political institution;
- the processing is necessary to achieve the aims of the institution;
- the political institution is in the process of being formed and the processing is necessary for this purpose;
- the processing is necessary to enable the data subject to take part in the activities of the institution;
- the processing is necessary to canvas for supporters or voters for a political party in the run-up to an election or referendum; or
- the processing is necessary for the purposes of campaigning for a political party or cause.

4.5.7. Specific authorisations for processing health or sex life



| Section 32 (Authorisation concerning data subject's health or sex life)

Information about health or sex life must always be treated as confidential. If the institution is not subject to a duty of confidentiality in law, a confidentiality agreement must be concluded with the data subject.

The information may only be shared with other institutions which are authorised to process the information and communication if the information is required by law or necessary for the performance of their duties.

Information concerning inherited characteristics may only be processed if a serious medical interest prevails or the processing is necessary for historical, statistical or research activities.

Medical professionals, healthcare institutions or social services may process information about a data subject's health or sex life if it is necessary for:

- the proper treatment of the data subject; or
- administrative purposes.

Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations may process information about a data subject's health or sex life if it is necessary to:

- assess the risk of the data subject to be 'insured' by the insurance company or medical scheme (unless the data subject has objected to the processing);
- perform in terms of an insurance or medical scheme agreement; or
- enforce any contractual rights and obligations.

Schools may process information about a data subject's health or sex life if it is necessary to provide special support or special arrangements for a pupil.

Any institution who manages the care of a child may process information about a data subject's health or sex life if it is necessary to carry out its lawful functions.

Any public body responsible for prison sentences or detention measures may process information about a data subject's health or sex life if it is necessary to implement prison sentences or detention measures.

Administrative bodies, pension funds, employers, or institutions working for them may process information about a data subject's health or sex life if it is necessary to:

- implement legislation, pension regulations or collective agreements that create rights that are dependent in the data subject's health or sex life; or
- reintegrate or support workers or persons who are entitled to benefits in relation to their sickness or work incapacity.

4.5.8. Specific authorisations for processing criminal behaviour or biometric information



Section 33 (Authorisation concerning the data subject's criminal behaviour or biometric information)

Criminal behaviour refers to the alleged commission of an offence as well as information about any proceedings relating to that alleged offence.⁸² Information about criminal behaviour must be distinguished from a data subject's criminal record. The latter relates to crimes for which the data subject has already been found guilty.

Institutions operating as employers are entitled to process information relating to criminal behaviour and biometric information as long as it is done in accordance with the rules established in labour legislation.

Personal information relating to criminal behaviour or biometric information can be processed by:

- bodies charged by law with applying criminal law; or

⁸² Section 26(b).

- institutions who have obtained the personal information in accordance with the law.



Example: Disciplinary records

The disciplinary records of students and employees may be seen as information relating to criminal behaviour if the student or employee committed a criminal offence.

4.5.9. When institutions may process the personal information of children



Section 34 (Prohibition on processing personal information of children)

Section 35 (General authorisations concerning personal information of children)

The default position is that institutions are prohibited from processing the personal information of children. However, POPIA provides a list of authorisations when the processing of the personal information of children is allowed.

Institutions will likely process the personal information of children when they:

- recruit prospective students;
- process student applications;
- provide teaching and learning services;
- manage employee benefits where a child may be the beneficiary; and
- do research.

Institutions must put measures in place to verify the age of data subjects. What measures are reasonable may depend on the risks inherent in the processing as well as the available technology.⁸³ Age verification must not lead to excessive processing of personal data.

4.5.9.1. Processing carried out with the prior consent of a competent person

The consent provided on behalf of a child must be a voluntary, specific and informed expression of will, as discussed in paragraph 4.5.1.6.



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

⁸³ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2026/679 Version 1.1 28.

A parent or legal guardian is a competent person who can provide consent on behalf of a child.⁸⁴ The High Court of South Africa is the upper guardian of all children. For children who do not have parents or a legal guardian, the court will step in and fulfil that role.⁸⁵

Institutions must ensure that the person who provides consent is in fact the parent or legal guardian of the child and must have measures in place to verify this. What measures are reasonable may depend on the risks inherent in the processing as well as the available technology. In low-risk cases institutions can verify that this is indeed the competent person via email and in high-risk cases it would be appropriate for an institution to ask for more proof.⁸⁶

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

4.5.9.2. Establishment, exercise or defence of a right or legal obligation

This authorisation allows institutions to process special personal information where it is necessary to exercise a right or claim that it has in terms of South African law, such as a right to access to information, a claim for money owed, property rights and contractual claims.

4.5.9.3. Obligation of international public law

Public international law has three main sources: customary international law, treaties and conventions. Section 39 of the Constitution requires that courts or other legal bodies must consider public international law when interpreting the Bill of Rights. The South African Constitution furthermore recognises international customary law as law in South Africa unless it is inconsistent with the Constitution or local legislation.⁸⁷ In addition, once an international treaty or convention has been approved by the National Assembly and the National Council of Provinces, South Africa is bound by them.⁸⁸

4.5.9.4. Historical, statistical or research purposes

Historical purposes include archiving and processing personal information of or concerning history or past events. In most cases, institutions will be required to process personal information for historical purposes by the National Archives and Record Services of South Africa Act,⁸⁹ in which case the institution will be authorised to process the information due to an obligation in law as discussed in paragraph 4.5.2.2.

Statistical purposes cover a wide range of processing activities, from commercial purposes to public interest.⁹⁰ It refers to any operation of collecting and processing information necessary for statistical surveys or for the production of statistical results.⁹¹

⁸⁴ Section 38 of the Children's Act 38 of 2005.

⁸⁵ Section 45 of the Children's Act 38 of 2005.

⁸⁶ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 28.

⁸⁷ Section 232 of the Constitution of the Republic of South Africa, 1996.

⁸⁸ Section 231 of the Constitution.

⁸⁹ Act 43 of 1996.

⁹⁰ Article 29 Data Protection working Party *Opinion 03/2013 on purpose limitation* 29.

⁹¹ Recital 162 of the European Union General Data Protection Regulation 2016/679.

Research purposes include the activities that are aimed at improving knowledge of any discipline through enquiry or systematic investigation, such as academic research, scientific research, commercial or industrial research, and technological development and demonstration.

To rely on this authorisation the responsible party must provide **sufficient guarantees** that the individual privacy of the data subject is not adversely affected, AND that EITHER processing is necessary to serve a [public interest](#); OR that to ask for consent appears to be impossible or would involve disproportionate effort (virtually impossible).

The **sufficient guarantees** that an institution must provide that the individual privacy of the data subject would not adversely be affected may include:

- having strict limitations on how much personal information is collected;
- immediately deleting the personal information that is not used;
- applying technical and organisational measures to keep personal information secure;
- anonymising the personal information;
- increasing transparency;
- providing an easy-to-use opt-out; and
- complying with an applicable issued code of conduct (e.g., Assaf POPIA Code of Conduct for research).

4.5.9.5. Deliberately made public with consent of competent person

The requirements to use the personal information of a child under this authorisation are that the information must have been:

- deliberately made public;
- by the child; AND
- with the consent of a competent person.

4.5.9.6. Authorisation by the Regulator

An institution may apply to the Regulator for authorisation to process the personal information of children. The Regulator may authorise the processing of personal information of children by publishing a notice in the Government Gazette if:⁹²

⁹² Information Regulator South Africa Guidance Note on Processing of Personal Information of Children 5.

- the processing is in the [public interest](#); AND
- appropriate safeguards have been put in place to protect the personal information of the child.

The appropriate safeguards referred to here are the technical and organisational security measures discussed in paragraph 4.9.⁹³

The Regulator may impose reasonable conditions for its authorisation, such as how the responsible party must:⁹⁴

- allow a competent person to review the processing of the personal information of children;
- allow a competent person to refuse to permit the further processing of the personal information of children;
- provide notice about the nature of the personal information of children that is processed;
- provide notice about how the information is processed;
- provide notice about further processing practices;
- refrain from any action that is intended to encourage or persuade a child to disclose more personal information than what is reasonably necessary for the purpose for which it is intended; and
- establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information of children.

4.5.10. When institutions may make automated decisions based on profiles



| Section 71 (Automated decision-making)

POPIA prescribes specific rules for automated decision-making based on profiles.

A **profile** is created when personal information is used to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that data subject's performance at work, credit worthiness, reliability, location, health, personal preferences and conduct.

A decision is considered 'automated' when no human judgement is involved.

If an automated decision that was based on a profile has legal or substantial consequences for the data subject, it triggers section 71 which means that institutions must comply with additional requirements.

⁹³ Information Regulator South Africa Guidance Note on Processing of Personal Information of Children 6.

⁹⁴ Information Regulator South Africa Guidance Note on Processing of Personal Information of Children 7.

Examples of automated decisions that are 'significant' for a data subject include decisions that:

- have a prolonged or permanent impact on the data subject;
- affect the behaviour and choices of the data subject;
- lead to discrimination and exclusion of the data subject;
- affect the data subject's financial circumstances (e.g., their eligibility for credit);
- affect the data subject's access to healthcare services;
- deny the data subject an employment opportunity or put them at a serious disadvantage; and
- affect the data subject's access to education (e.g., university admission).

Automated decisions based on profiles are allowed if the decision is:

- taken in connection with the conclusion or execution of a contract and;
 - the request of the data subject in terms of the contract has been met; or
 - appropriate measures have been taken to protect the data subject's legitimate interests; or
- governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of the data subject.



Example:

An institution has an automated student application process. The prospective student completes an extensive application form online, a profile is created of the prospective student and based on this profile, some prospective students are automatically accepted. The request of the data subject have been met in this example and the institution may use this manner of automated decision-making based on profiles.

If the prospective student was automatically declined the institution must implement appropriate measures to protect the data subject's legitimate interests as described below.



Recommendation:

To protect the data subject's legitimate interests with automated decision-making, Institutions should:

- implement a policy framework for the use of personal information of data subjects in automated decision-making that allocates specific roles and responsibilities for:
 - collecting the personal information to be used;

- anonymising the personal information where appropriate;
- performing the analytics processes on the personal information and the purpose of the processes;
- making decisions based on the analysis (e.g., in learner analytics, who is responsible for the interventions); and
- retaining and having custodianship of personal information used or created during the automated decision-making process;
- conduct a PIIA before implementing automated decision-making processes, including consulting with affected data subject groups and representatives;
- ensure that algorithms used in automated decision-making are peer-reviewed;
- ensure that the institutions are transparent about automated decision-making and the algorithms that are used;
- assess the quality of personal information used in automated decision-making processes;
- provide all data subjects who are subject to automated decision-making with meaningful access to the personal information used and created and the opportunity to make representations to the institutions about the decision;⁹⁵
- ensure that inaccuracies in the information used in and created by automated decision-making processes can be identified, reported, analysed and remedied;
- minimise adverse impacts to ensure, for example, that trends, norms, categorisation, or any labelling of students do not bias staff, students or institutional perceptions and behaviours towards them; and
- ensure that all staff are trained and have a working understanding of legal, ethical, and unethical practices.

4.5.11. When institutions may process personal information for a new purpose



| Section 15 (Further processing to be compatible with purpose of collection)

New purposes for collecting personal information may emerge, or the purpose may change after the personal information was collected. When this happens, institutions must assess whether a new justification is required to make the processing activity lawful. POPIA's further processing limitation requires institutions to establish whether the new purpose is in accordance with or compatible with the

⁹⁵ There may be circumstances where access may be harmful for data subjects. Institutions must ensure that they have clear policies that regulate access to this information as well as instances where access will be withheld.

purpose for which the personal information was collected in the first place. If the further processing is not compatible, the processing is unlawful.

To demonstrate compatibility, the new purpose behind the further processing must either:

- be generally compatible; or
- meet the criteria for one of the automatic justifications.

4.5.11.1. Assessing general compatibility with the original purpose

Institutions must take certain factors into account to determine whether a new purpose for further processing is compatible with the original purpose for processing. Institutions must consider the following:

- The relationship between the original purpose and the new purpose. If the new purpose was implied in the original purpose (e.g., it was a logical next step), it will be compatible, however if the new purpose is very different from the original purpose or would be an unexpected change, it is likely that the further processing is incompatible.
- The nature of the information concerned. Institutions must evaluate whether the new purpose requires the processing of sensitive information, because sensitive personal information (e.g., a child's information or health information) justifies higher levels of protection, the test for compatibility with the original purpose will be stricter.⁹⁶
- The consequences that the further processing would have for the data subject. If the new purpose would have a large or substantial negative impact on the data subject, it is likely that the further processing is incompatible.
- The manner in which the personal information was collected. The information and notifications provided to the data subject at the point of collection inform the reasonable expectations of the data subject. If the data subject could reasonably expect further processing on the basis of the information and notifications, it is likely that the further processing is compatible.
- Any contractual rights between the data subject and the responsible party. If further processing is necessary to perform the responsible party's rights and obligations in terms of a contract, it is likely that the further processing is compatible.

⁹⁶ Article 29 Data Protection Working Party *Opinion 3/2013 on purpose limitation* 21.

**Example:**

An institution uses a student's results to consider the student for funding even though the student did not apply for funding. This further processing is likely to be compatible because providing funding to students is one of the university's main objectives and the outcome will either have no impact on the student, or if the student receives funding, be positive.

4.5.11.2. When processing for a new purpose is automatically justified

Further processing will be automatically justified if:

- the data subject consented to the new or changed purpose;
- the personal information is available in or derived from a public record;
- the personal information was deliberately made public by the data subject;
- the further processing is necessary to avoid prejudice to the maintenance of law by any public body which includes the prevention, detection, investigation, prosecution and punishment of offences;
- the further processing is necessary to protect the interest of national security;
- the further processing is necessary to perform a legal obligation or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Services Act;
- the further processing is necessary to conduct proceedings in any court or tribunal that have commenced or are reasonably contemplated;
- the further processing is aimed to prevent or mitigate a serious or imminent threat to public health or the life or health of an individual;
- the personal information is used for historical, statistical or research purposes and the responsible party ensures that the further processing will only be done for this purpose and that the results will not be published in identifiable form; or
- the Information Regulator has granted an exemption.

**Example:**

During the COVID-19 pandemic institutions had to introduce measures that required further processing of students', employees', and members of the public's personal information. The further processing was justified to prevent or mitigate a serious threat to public health and to individuals' life or health.

An institution wants to publish individual graduation photos on Facebook for marketing purposes. These photos were initially taken for purposes of selling the photos to the students and for record-keeping purposes. The new purpose (marketing on Facebook) was not envisaged at the time that the photos were taken and publishing them would not be

compatible with the original purpose. The institution must obtain the students' consent before using their photos for the new purpose.

4.5.12. When institutions need prior authorisation to process personal information



Section 57 (Processing subject to prior authorisation)

Section 58 (Responsible party to notify the Regulator if processing is subject to prior authorisation)

There are some instances where an institution must obtain authorisation from the Regulator before processing personal information. This requirement allows the Regulator to have oversight and control over certain high-risk activities.

4.5.12.1. When prior authorisation is required

Institutions must obtain prior authorisation from the Regulator if they plan to:

- process unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection and with the aim of linking the information with information processed by other responsible parties;⁹⁷



Unique identifier means any identifier assigned to a data subject that a responsible party uses for the purposes of the operation of that responsible party and that uniquely identifies that data subject in relation to that responsible party. Examples of unique identifiers include account numbers, policy numbers, identity numbers, employee numbers, student numbers, telephone or cell phone numbers, or reference numbers.⁹⁸

- process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;⁹⁹
- process information for credit reporting (e.g., credit bureaus);

⁹⁷ Neither POPIA nor the Regulator's Guidance Note on application for prior authorisation explains what 'linking' means. Some experts are of the opinion that a new data set must be created and that the new 'linked' dataset must be available to both responsible parties. See De Stadler, Luttig Hattingh, Esselaar and Boast *Over-thinking the Protection of Personal Information Act* 243

⁹⁸ Information Regulator (South Africa) Guidance note on application for prior authorisation 5.

⁹⁹ This section applies to responsible parties conducting criminal record enquiries, reference checks pertaining to the past conduct, or disciplinary action taken against a data subject. Information Regulator (South Africa) *Guidance note on application for prior authorisation* 5.

- transfer the special personal information or personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information;¹⁰⁰ and
- process any other type of information processing by law or regulation which the Regulator may consider carrying a particular risk for the legitimate interests of the data subject as published by the Regulator from time to time.

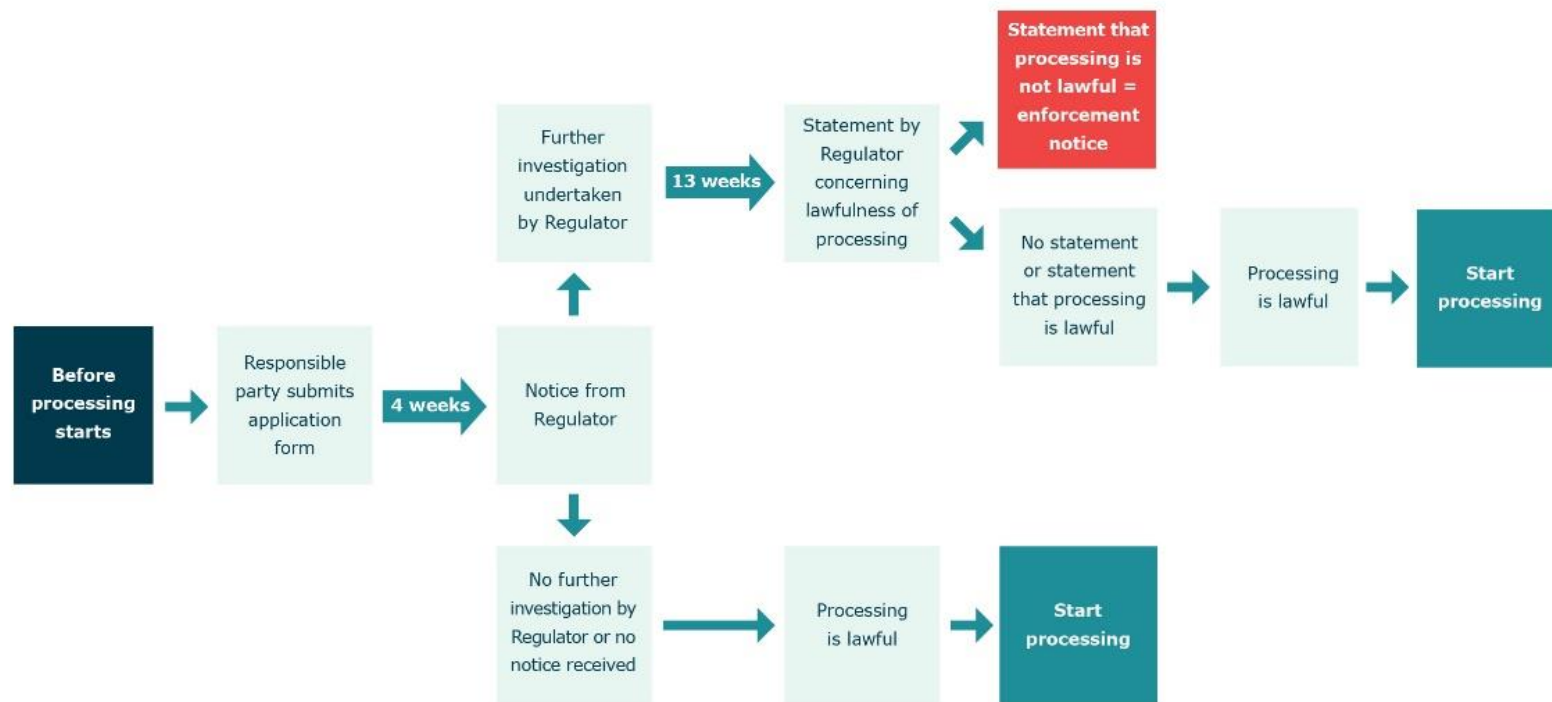
Prior authorisation is not required when an institution is subject to a code of conduct issued by the Regulator.

4.5.12.2. How institutions may apply for prior authorisation

Institutions may apply for prior authorisation using the [application form](#) published by the Regulator and following the process described in the Guidance Note on application for prior authorisation. POPIA prescribes timelines by which the Regulator must respond to an application. If the responsible party does not receive a response by the deadline, they can assume that the processing is lawful and start the processing activity. Here is a visual representation of the process and timelines:

¹⁰⁰ A third party provides an adequate level of protection if it is subject to a law, binding corporate rules or binding agreement which effectively upholds principles substantially similar to POPIA's eight conditions for the lawful processing of personal information. Information Regulator (South Africa) *Guidance note on application for prior authorisation* 6.

Figure 5: How institutions may apply for prior authorisation



4.5.12.3. Consequences of not obtaining prior authorisation



Section 59 (Failure to notify processing subject to prior authorisation)
Section 107 (Penalties)

A failure to apply for prior authorisation when it is required or to comply with the rules regarding how prior authorisation may be requested is a criminal offence. The institution may be fined (up to R10 million) or face imprisonment of up to 12 months, or both.

4.6. INSTITUTIONS MUST COLLECT PERSONAL INFORMATION FROM THE DATA SUBJECT



Section 12 (Collection directly from the data subject)

The default rule in POPIA is that institutions must always collect personal information directly from the data subject.

However, section 12(2) of POPIA contains several exceptions to this default rule. Should institutions want to rely on these exceptions, they must review their sources of personal information regularly and keep a record of the exception they rely on when not complying with the default rule.

4.6.1. Institutions must collect personal information directly from the data subject

The default position is that institutions must collect personal information directly from the data subject. There are two main reasons for this rule, namely that:

- when personal information is collected from the data subject, the data subject is usually aware of the collection and has (some) control over what information is provided; and
- the data subject will in most cases be the most reliable source of information.

Sometimes it is impossible for the institution to collect personal information directly from a data subject. The institution must then establish if there is a justification in terms of POPIA to collect personal information from third-party sources. POPIA provides several exceptions to the default rule.

4.6.2. When institutions may collect personal information from other sources

When any of the justifications apply, it is lawful for the institution to collect personal information from a source other than the data subject. However, it is still a requirement that the institution must have a legal justification to process the personal information, notify the data subject of the collection, and comply with all the other requirements for the lawful processing of the personal information.

4.6.2.1. Personal information in or derived from a public record

An institution may collect personal information that is contained in or derived from a public record.



Public record means a record that is accessible in the public domain and which is in the possession or under the control of a public body, whether or not it was created by that public body.



Examples of public records include the deeds registry, information on a university's website, and information found at the Companies and Intellectual Property Commission (CIPC).

4.6.2.2. Personal information which the data subject deliberately made public

An institution may collect personal information if the data subject deliberately made that information public.

To rely on this exception the institution must be cautious and prove or be certain that the data subject themselves made the information public. For instance, when a person's information is published by their contacts on social media, by their employers on a company website, or by journalists in news media, the institution must first establish if the data subject deliberately made that information publicly available.



Example:

A person's publicly available LinkedIn profile (i.e., you don't have to be a connection to see the information).

4.6.2.3. The data subject has consented to collection from another source

An institution may ask the data subject for consent to collect personal information from a third party. For the consent to be valid, it must be voluntary, specific and informed. See the requirements for valid consent discussed in paragraph 4.5.1.6.



Example: Advertising cookies

An institution may ask website visitors to give consent for the use of advertising cookies. Advertising cookies track user behaviour on a website and are used to personalise the user's experiences and to display targeted advertising. If a data subject is interested in receiving targeted advertising, they could either tell the institution what they are interested in, or consent to the use of cookies that collect information about them and their online behaviour.

4.6.2.4. No prejudice to the legitimate interest of the data subject

If an institution can demonstrate that collecting the personal information from another source does not prejudice a legitimate interest of the data subject, it can go ahead with the collection.



Example: Medical emergency

An institution may collect personal information from third-party sources if it is necessary to treat the data subject in a medical emergency or to ensure the safety of data subjects.

4.6.3. When institutions create personal information

Institutions create personal information of students, employees, visitors and others when they create records, such as records of class attendance, access logs, performance reviews, examination results

and disciplinary hearings. Very often data subjects are unaware of this information. Despite this, data subjects still own their personal information.¹⁰¹

Institutions must comply with all POPIA requirements when creating and processing personal information. For instance, institutions must notify the data subjects if they process personal information and must allow data subjects to exercise their rights to request access, correction, and deletion.

4.7. INSTITUTIONS MUST NOTIFY DATA SUBJECTS OF PROCESSING



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

POPIA requires responsible parties to be transparent about the processing of personal information. The aim is to enable data subjects to understand how processing takes place and to give them a way of exercising control over their information.

4.7.1. What institutions must disclose to data subjects



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

Section 14 of PAIA (Manual on functions of and index of records held by a public body)

Institutions must notify data subjects of:

- the information being collected;
- the source from which the information is collected;
- the name and address of the institution;
- the purpose(s) for which the information is being collected;
- whether the supply of the personal information by the data subject is voluntary or mandatory;
- the consequences if they fail to provide the information;
- any particular law authorising or requiring the collection of the information;

¹⁰¹ The ownership of personal information came to the fore in the case of *Discovery Ltd v Liberty Group Ltd* 2020 (4) SA 160 (GJ), where it was common cause that a Vitality member's Vitality status does not form part of Discovery's confidential, proprietary information. Instead it is the members' personal information, and Vitality members are free to make it public, and to disclose it to Liberty. However, the underlying science, proprietary algorithms, data and modelling underpinning the Vitality programme that are used to determine members' Vitality status, are confidential information and proprietary to Discovery, and protected by the Copyright Act.

- the institution's intent to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;
- a general description that allows a preliminary assessment of the suitability of the information security measures that the institution will implement to ensure the confidentiality, integrity, and availability of the information;¹⁰²
- the recipients or category of recipients;
- the nature or category of the information;
- the existence of data subject rights; and
- the contact details of the Regulator.

Why institutions should not ask for consent in their privacy notices.

A privacy notice is not the appropriate place to ask a data subject for consent to process their personal information, because:

- a privacy notice is a notification, not an agreement, which means that the data subject does not have to 'accept' the privacy notice, it is merely information that is made available to the data subject; and
- if the wording in a privacy notice implicates that a form of consent is hidden in that privacy notice it will not fulfil the requirements of a valid consent as discussed in paragraph 4.5.1.6 of this Guideline.

4.7.2. When must institutions notify data subjects



| Section 18 (Notification to data subject when collecting personal information)

The general principle is that notification cannot take place after the fact, in other words the data subject must be informed when personal information is directly collected from them. For instance, if the collection is taking place via a web-based form, the privacy notice should be accessible on the same page where the personal information is collected.

If, however, information is collected from another source, the data subject must be informed about the collection as soon as reasonably practicable after collection.

¹⁰² This requirement is not in section 18 of POPIA but is required by section 14(2)(v) of PAIA.

What does ‘as soon as reasonably practicable’ mean?

POPIA is silent on what ‘as soon as reasonably practicable’ means and the Regulator has not published guidelines on the subject. The following has been found in other jurisdictions:

- In Kenya, controllers must notify data subjects within 14 days of indirect collection.¹⁰³
- According to the EU GDPR, notification of collection must be made within a ‘reasonable period’ after collection and no later than one month, having regard to the specific circumstances in which the personal data is processed. If the personal data is being used to communicate with the data subject, notification must be made at the latest with the first communication. If the first communication happens more than one month after collection, the notification must happen by latest one month.¹⁰⁴

If the purposes for which personal information is processed change, the institution must update the privacy notice and proactively bring the changes to the attention of the affected data subjects before the processing for a new purpose starts.

If an institution cannot comply with the transparency requirement in time, it must document the reason for non-compliance.

4.7.3. How must institutions notify data subjects

POPIA requires that responsible parties must take ‘reasonably practicable steps’ to ‘ensure that the data subject is aware of all of the required information.

When drafting a privacy notice, institutions must ensure that the notice is written in a clear and concise manner. The EU GDPR requires that the notice must be given in a ‘concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particularly for any information addressed specifically to a child.’¹⁰⁵ This definition is very similar to the definition of ‘plain language’ in section 22 of the Consumer Protection Act 68 of 2008 that applies to contracts with students.

¹⁰³ Regulation 6(3) of *The Data Protection (General) Regulations, 2021* published in the Kenya Gazette Supplement No. 236 of 31 December 2021.

¹⁰⁴ Article 14 of the EU GDPR and Article 29 Data Protection Working Party *Guidelines on transparency under Regulation 2016/679* 15.

¹⁰⁵ Article 12(1) of the EU GDPR.

The language must be appropriate for the intended audience.¹⁰⁶ If, for instance, an institution must draft a privacy notice intended for prospective students, the institution should consider that the prospective students are mostly still minors without the same level of education and sophistication as an adult.¹⁰⁷

Privacy notices must be easily accessible and may be provided in a range of ways, such as:

- orally – face to face, or when speaking on a phone;
- in writing – printed media or forms (e.g., on the student application form or job applicant form);
- through signage – an information poster in a public area (e.g., a notice at the campus entrance about CCTV monitoring); and
- electronically – in text messages, on websites, in emails and mobile apps.¹⁰⁸

If an institution considers collecting or creating personal information using artificial intelligence (AI) the potential impact on the right to privacy of data subjects, must be assessed. Individuals often have limited awareness of their personal information being collected in this way. If necessary, institutions must add additional detail to their privacy notices about these activities, making sure to bring it to the attention of data subjects. It could be useful to use just-in-time notices to deliver this type of information.¹⁰⁹ If AI is used to make automated decisions based on profiles, institutions must provide additional information as discussed in paragraph 4.5.10.

4.7.4. When institutions are exempt from notifying data subjects

POPIA provides some exemptions to institutions concerning the notification to data subjects of the processing of their personal information. Section 18(4) provides that institutions do not have to notify data subjects that their personal information is being processed if:

¹⁰⁶ The European Article 29 Data Protection Working Party articulated the plain language requirement in respect of children and other vulnerable groups as follows: 'Where a data controller is targeting children or is, or should be, aware that their goods/services are particularly utilised by children ... it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/information is being directed at them. A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language". Equally, if a data controller is aware that their goods/services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects.' Article 29 Data Protection Working Party *Guidelines on transparency under Regulation 2016/679* 10.

¹⁰⁷ The Dutch Data Protection Authority fined TikTok 750 000 Euro for violating the privacy of Dutch children because the privacy information was only available in English and not also in Dutch. Read more about the finding at: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en.

¹⁰⁸ The UK Information Commissioner's Office *UK GDPR guidance and resources on individual rights - the right to be informed* available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>.

¹⁰⁹ The UK Information Commissioner's Office *UK GDPR guidance and resources on individual rights - the right to be informed* available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-common-issues-might-come-up-in-practice/>.

- the data subject consented to not being notified;



Example: Training generative AI technologies

The data subject consents to their information being used to train generative AI technologies without notification of each processing activity and purpose.

- not notifying the data subject will not prejudice the legitimate interests of the data subject;



Example: Emergency

An institution may process a student's personal information without notification if it is an emergency situation and necessary to ensure the safety of the student.

- not notifying is necessary:
 - to avoid prejudice to the maintenance of the law by any public body;
 - to comply with a legal obligation or to enforce legislation concerning the collection of revenue by the South African Revenue Services (SARS);
 - to conduct proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
 - in the interests of national security;



Example: Court proceedings

It is not necessary to notify a creditor when an institution is collecting their personal information to institute proceedings in a court to collect a debt owed to the institution.

- notifying the data subject would prejudice a lawful purpose of collection;



Example: Fraud prevention

It is not necessary to notify the data subject when an institution is investigating suspected fraud.

- notifying the data subject is not reasonably practicable;



Example: Impractical to notify

It is not necessary to notify the data subject if the institution does not have the data subject's contact information.

- the information will not be used in a form in which the data subject will be identified; or



Example: Data subjects not identified

An institution collects information of the device used to access its website and the visitor's IP address through the use of cookies. The institution uses this information to optimise their website and have no intention of identifying website visitors.

- the information will be used for historical, statistical or research purposes.

4.7.5. What information must institutions provide in a PAIA manual

Institutions must make a PAIA manual easily available in three official languages following the template provided by the Regulator.¹¹⁰ PAIA manuals must at least be available:

- on the institution's website; and
- at the reception area of the institution during business hours.

4.8. INSTITUTIONS MUST ENSURE THE QUALITY OF PERSONAL INFORMATION



| Section 16 (Information quality)

Institutions must take reasonable steps to ensure that the personal information it has is of a good quality. The reasonable steps institutions must take will depend on the context, for example:

- If the personal information is going to be used to make important decisions about the data subject, the institution is under a greater duty to ensure that the information is correct.
- If the personal information was collected from a source other than the data subject, the institution cannot assume that the information is correct and may be required to take steps to verify the information.

To consider information to be of a 'good quality' the personal information must be:

- complete;
- accurate;
- not misleading; and
- updated when necessary.

¹¹⁰ Section 14(1) of PAIA. The Regulator's template for public bodies is available at: <https://info regulator.org.za/wp-content/uploads/2020/07/PAIA-Manual-Template-Public-Body.pdf>.

4.8.1. Personal information must be complete

A record can be accurate, but incomplete. This is very important when personal information is used to make decisions about the data subject such as the information given on a student application form. Institutions must take reasonably practicable steps to ensure that they have all the information required for the processing activity, while keeping the principle of minimality in mind.

4.8.2. Personal information must be accurate

Accuracy refers to the correctness of the record. Whether an institution must take active steps to keep personal information accurate will depend on the purpose for which it is used and how severe the consequences would be if the information is incorrect. For instance, contact details should generally be kept up to date to ensure that students, employees, or alumni continue to receive communications from an institution. It would be reasonable, for example, for a university to ask these data subjects to update their details, but the university does not have to take extreme measures, such as independently verifying the information, to establish that it has the correct information.

However, if the record is intended to be historical, the fact that the personal information in that record has since changed, does not mean that the historical record is now inaccurate and must be deleted.

If the intention is to keep a historical record, that intention must be clear, and a safeguard must be put in place to prevent the historical record from being used for any other purpose.

4.8.3. Personal information must not be misleading

Personal information that is not kept up to date could be misleading. This may have dire implications for data subjects and may affect the service delivered to them.

For instance, opinions about a person are considered to be personal information. Opinions are inherently subjective and not intended to present facts. This means that even if a data subject disagrees with an opinion or if the opinion is later disproved, the opinion is still considered accurate unless it was based on inaccurate data. However, it would be misleading if the institution's records did not clearly indicate that this was a data subject's opinion and even whose opinion it was.¹¹¹

4.8.4. Personal information must be updated where necessary

To ensure the quality of personal information, it must be updated. When institutions learn about a mistake or inaccuracy in personal information, they must take steps to rectify that information. The steps that the institution must take would depend on the circumstances, the type of personal information involved, and the purpose for which the information was used.

Data subjects have the right to contest the accuracy of their personal information. See paragraph 4.13.3.

In some cases it is reasonable to rely on the data subject to notify the institution when their personal information has changed, such as when their contact details change. However, it is not the data subject's duty to update their personal information. For instance, if an email address is not working and the institution receives a report to this effect, the institution must either take steps to correct the email

¹¹¹ See <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/>

address or indicate in its records that it is outdated. It may be sensible for institutions to ask data subjects to update their own details periodically.¹¹²

4.8.5. Personal information from third-party sources must be verified or updated

It has become commonplace to verify the accuracy of personal information and update it in large batches by comparing the information with publicly available information. This is typically done by third parties on behalf of institutions. For instance, a university may use public records to improve the quality of the contact details it has of its alumni or it may instruct a third party to do so on its behalf.

It will be justified if the institution wants to verify personal information that it already has or if the institution wants to improve the accuracy of the information as long as the use of a third-party source is justified on one of the grounds set out in section 12(2). This was discussed in paragraph 4.6.2. When the purpose of the collection is to verify or update personal information, the most common justifications will be that:

- it would have been impractical to verify the information with the data subject directly – either because it would be too expensive to verify the records individually, or because the contact details of the data subject are out of date;¹¹³
- the personal information used in the verification is contained in or derived from a public record or has deliberately been made public by the data subject;¹¹⁴
- the verification of the personal information from another source is necessary to maintain the legitimate interests of the institution;¹¹⁵ or
- the institution asked for the consent of the data subject to verify their information,¹¹⁶ for example, when the institution requests consent from the data subject for verifications through credit bureaus or verification agencies.

If the institution is compiling personal information from sources other than the data subject, verification from the data subject may be needed to ensure that the personal information is accurate. Verification of information obtained from sources other than the data subject will be required if inaccuracies would have serious consequences for the data subject. For instance, the financial information that an institute considers in order to decide whether to give a student funding should be both independently verified and confirmed by the data subject.

¹¹² See <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/>.

¹¹³ Section 12(2)(f).

¹¹⁴ Section 12(2)(a).

¹¹⁵ Section 12(2)(d)(iv).

¹¹⁶ Section 12(2)(b).

4.9. INSTITUTIONS MUST ENSURE THE SECURITY OF PERSONAL INFORMATION

4.9.1. What institutions must protect personal information against



Section 19: (Security measures on integrity and confidentiality of personal information)

Institutions must safeguard the personal information of data subjects against:

- damage;
- loss;
- loss of access;
- unauthorised access;
- unauthorised destruction; and
- unauthorised use.



Examples of information security breaches:

- Employee or human error. This includes misconfiguration, mistaken delivery and publishing errors, including the classical mistake of sending an email to the wrong person.
- Malicious insiders. This happens when people who have access to systems and information use that information with malicious intent.
- Malware. This includes password dumpers, phishing emails and ransomware.
- Data loss. This includes accidental loss of information and the incorrect application of records retention requirements.
- Hacking. Hacking includes those using stolen or brute force credentials, those exploiting vulnerabilities, and those that attack using backdoors or Command and Control functionality.
- Social engineering. This happens when someone convinces an institution to give them information or access to information that they must not have.
- Theft. Physical theft of devices or records containing personal information.
- Unlawful processing. This happens when someone uses personal information without a legal justification. For instance, when an institution uses prospective students' information for direct marketing without first obtaining consent.

According to POPIA, institutions must implement both technical and organisational measures to protect personal information. Technical measures include firewalls, anti-virus software, encryption, masking and pseudonymisation. Organisational measures include policies, procedures, and training.

4.9.2. How institutions must manage information security risks

Section 19(2) requires institutions to take reasonable measures to:

- identify risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are properly implemented; and
- regularly update safeguards in response to new risks or deficiencies in existing safeguards.

Section 19(3) says that a ‘responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of a specific industry or professional rules and regulations.’ There are many examples of generally accepted information security practices and procedures, such as ISO/IEC 27000: Standards for an information security management system, ISO 22301: Business Continuity Management Systems, ITIL (The Information Technology Infrastructure Library), the NIST Cybersecurity Framework and COBIT (Control Objectives for Information Related Technologies).¹¹⁷



Recommendation:

There are various measures that institutions can take, institutions should at least:

- create and implement appropriate business continuity and IT disaster recovery standards, information security management policies and supporting procedures, such as an information security incident response procedure;
- implement information security policies and procedures through training;
- analyse the risks inherent to processing personal information and implement appropriate controls to mitigate those risks;
- align its information security management efforts with generally accepted information security practices and procedures; and
- regularly test and review information security measures, and where necessary, improve them.

¹¹⁷ The Information Regulator has referenced ISO/IEC 27001, the Public Service Corporate Governance of Information and Communication Technology Framework, and the Payment Card Industry Data Security Standards as examples of generally accepted information security practices and procedures in enforcement notices issued in 2023 and 2024. Available at: <https://info regulator.org.za/enforcement-notices/>.

4.9.3. How institutions must manage security compromises



Section 22 (Notification of security compromises)

Institutions must notify the data subjects and Regulator of certain types of information security breaches. A notifiable security compromise is 'where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person'.

If an institution experiences a notifiable security compromise it must notify the Information Regulator as soon as possible (within 72 hours) using the prescribed form.¹¹⁸ Institutions can, however, delay notifying the Regulator if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that such a notification will impede a criminal investigation.

Institutions must also notify all affected data subjects if they can be identified. The notification must be in writing and communicated in at least one of the following ways:

- by mail;
- by email;
- in a prominent position on the institution's website;
- published in news media; or
- as directed by the Regulator.¹¹⁹

The notification must provide information to allow the data subject to take protective measures against the potential consequences of the compromise. This information could include:

- a description of the possible consequences of the compromise;
- a description of the measures the institution have taken or will take to address the compromise;
- a recommendation of measures that the data subject can take to mitigate the adverse effects of the compromise; and

¹¹⁸ Available at: <https://infoeregulator.org.za/wp-content/uploads/2020/07/FORM-SCN1-Security-Compromises-Notification-Fillable-Formpdf.pdf>. The Regulator published Guidelines on completing the form available at: <https://infoeregulator.org.za/wp-content/uploads/2020/07/Guidelines-on-completing-a-Security-Compromise-Notification-ito-Section-22-POPIA.pdf>. POPIA does not give a deadline for reporting to the Regulator, but the Regulator has indicated that they expect responsible parties to report a security compromise within 72 hours.

¹¹⁹ In the enforcement notice issued against the SAPS, the Regulator also required the SAPS to publish an apology to data subjects in all major weekly newspapers and in all social media platforms such as Facebook and Twitter. The enforcement notice is available at: <https://infoeregulator.org.za/wp-content/uploads/2020/07/ENFORCEMENT-NOTICE-SAPS-MATTER-04052363.pdf>.

- if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

If a security compromise happens at an operator of the institution, the operator must notify the institution immediately. The institution, as responsible party, remains responsible to notify its data subjects and the Regulator.

IMPORTANT: Institutions must develop and implement incident response plans that incorporate the notification requirements.

4.10. USING AN OPERATOR TO PROCESS PERSONAL INFORMATION ON AN INSTITUTION'S BEHALF



Section 20 (Information processed by an operator or person acting under authority)

Section 21 (Security measures regarding information processed by operator)

4.10.1. How to identify operators and what they are accountable for

Paragraph 3.1 discusses how to identify operators. Operators only have some direct responsibilities regarding the processing of personal information.

In terms of POPIA, operators:

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

4.10.2. Institutions must have written contracts with operators

POPIA requires that there must be a written agreement between the institution and their operator and that this agreement must state that the responsible party would ensure that the operator establishes and maintains appropriate technical and organisational security measures. This is the only obligation that must be recorded in a written agreement with operators.



Recommendation:

When institutions draft and review agreements with their operators, the institutions must ensure that the agreement:

- identifies the Information Officers;
- describes the purposes for which the operator may process personal information;
- limits the purposes for which the operator may use the personal information to instances the institution has authorised the operator;

- demands that the operator must keep the personal information confidential and not share it with third parties without the institution's written approval;
- reserves the right that the institution can demand the return or destruction of personal information;
- describes how the operator must deal with requests and complaints from a data subject, or notices, requests and complaints from the Regulator;
- describes the information and cyber security measures that the operator must have in place;
- describes the process that the operator must follow when they experience a security compromise;
- includes obligations, if the operator is situated outside South Africa, to ensure the operator provides an adequate level of protection that effectively upholds the principles for the reasonable processing of the information that are substantially similar to the principles of POPIA;¹²⁰
- includes a right to audit the operator's compliance with POPIA and the security requirements, when appropriate; and
- considers whether indemnities and limitations of liability is appropriate.

4.11. WHEN INSTITUTIONS MUST DELETE OR DESTROY PERSONAL INFORMATION



| Section 14 (Retention and restriction of records)

Institutions must only retain personal information for as long as it is necessary to achieve the purpose of collection, and no longer. However, institutions can retain records for longer periods if:

- it is required by a law;¹²¹
- the institution requires the record for lawful purposes related to their functions or activities;
- a contract requires the retention;
- the data subject gave consent that the institution may retain their information;

¹²⁰ Section 72 (Transfer of personal information outside Republic of South Africa)

¹²¹ For instance the National Archives and Records Service of South Africa Act, the Copyright Act, Higher Education Act, and the Promotion of Administrative Justice Act.

- the institution is keeping the record for historical, statistical or research purposes as long as the institution ensures that the record is not used for any other purpose; or
- if the institution made a decision about a data subject based on a certain record, the record must be retained as prescribed by law, a code of conduct, or for a period which will afford the data subject a reasonable opportunity to request access to the record.



Recommendation:

Institutions should create and implement a records retention schedule that contains:

- a list of the categories of records that must be maintained for legal, regulatory, historical and operational requirements;
- a default retention rule for each category of records;
- any exceptions to the default rules for specific records within a category;
- the legal, regulatory, historical, or operational requirement that necessitates the retention of a category of records or a specific record;
- the period for which the category of records or specific record must be retained; and
- the event that triggers the start of the period.

Institutions must destroy or de-identify personal information as soon as reasonably practical after it no longer has any justification to retain the personal information. A record will be considered deleted or destroyed if it has become impossible to reconstruct the record in an intelligible form.

Personal information is considered de-identified if all information is deleted that:¹²²

- identifies the data subject;
- can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- can be linked by a reasonably foreseeable method to other information that identifies the data subject.

¹²² Definition of 'de-identify' in Section 1.

4.12. WHEN INSTITUTIONS MUST RESTRICT THE PROCESSING OF PERSONAL INFORMATION



| Section 14 (Retention and restriction of records)

POPIA requires that the processing of personal information must be restricted if:

- the accuracy of the personal information is contested by the data subject and it must be restricted for the time that the institution investigates the accuracy of that personal information;
- the institution no longer needs the personal information to achieve the purpose for which it was collected in the first place but is retaining it as proof or for historical purposes, then the institution must not process the personal information for any other reasons;
- the institution was processing the personal information without a legal basis,¹²³ then the data subject can request that the information must be restricted instead of being destroyed; or
- the data subject requests that the information be transmitted to another automated processing system.

Restricting processing means that personal information may not be processed other than it being stored. This usually means that the institution must:

- temporarily move the information to another (inactive) processing system;
- make the information unavailable to users; or
- temporarily remove published data from a website.

There are some exceptional circumstances when an institution may process personal information despite a restriction, for instance if:

- the information is processed for the purpose of truth;
- the data subject consents to the processing;
- the information is processed to protect the rights of another individual or organisation; or

¹²³ See the legal justifications available to institutions in section 4.5.

- the processing is in the public interest.¹²⁴

4.13. HOW INSTITUTIONS MUST RESPECT DATA SUBJECT RIGHTS



Section 5 (Rights of data subjects)

Data subjects have the right to have their personal information processed in accordance with the conditions for the lawful processing of personal information. This right includes that the data subject:

- be notified;
- have access to their personal information;
- may correct their personal information;
- may request the deletion or destruction of their personal information;
- may object to processing; and
- may opt out or unsubscribe from direct marketing.

Each right is discussed in more detail in the rest of this section.

4.13.1. Data subjects' rights to be notified



Section 18 (Notification to data subjects when collecting personal information)

Section 22 (Notification of security compromises)

Data subjects have the right to be notified when their personal information is being collected. This requirement is discussed in section 4.7.

Data subjects must be notified when their personal information was accessed or acquired by an unauthorised person (security compromise). This requirement is discussed in section 4.9.3.

4.13.2. Data subjects' right to access their personal information



Section 23 (Access to personal information)

Data subjects have the right to request an institution to:

¹²⁴ Processing in the public interest is discussed in section 2.2.1.1.

- confirm whether or not it holds personal information about them;
- provide a record or a description of their personal information in the institution's possession; and
- provide information about the identity of all third parties, or categories of [third parties](#), who have, or have had, access to their personal information.

The form that data subjects may use to request access to their personal information is the same form that must be used for making PAIA requests.¹²⁵ This can be very confusing and institutions must check each request to determine whether it is a data subject request. These are the different types of requests institutions may receive and how to distinguish them:

Who is sending the request?	Why are they sending the request?	Principles to apply or processes to follow
An employee, student, third party or any other data subject.	The data subject is sending requests about their personal information.	This is a data subject access request and institutions must follow the process described below.
Any other person or organisation.	To access institutional information.	Follow the institution's PAIA manual.
An employee of the institution.	To access institutional information to do their job.	Follow the institution's internal access control procedure.

If it is a data subject request, the institution should follow the following process to respond:¹²⁶

- Determine if the institution is the responsible party by identifying the activities where the personal information is being processed and follow the assessment described in section 3.1.
- Confirm the identity of the data subject, for instance, ask for the student number and whether the student was enrolled for a particular subject.
- Request more information if necessary to find their personal information.
- Determine what information the institution has. If the data subject requests a copy of their record the institution must redact any information concerning third parties or information that the institution has a valid reason to refuse access to and information that does not fall within the definition of personal information of the requester.

¹²⁵ Form 2 is available at: <https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-PAIA-Form02-Reg7.pdf>

¹²⁶ Despite the process being described as seven distinctive steps, most of these activities can happen concurrently and can be followed in a different sequence.

- Consider whether the institution has grounds to refuse the request. Institutions can rely on any of the grounds set out in Chapter 4 of PAIA.
- Determine the fee and provide a written estimate to the data subject before processing the request.¹²⁷
- Provide the response regarding the institution's decision by using Form 3.¹²⁸

4.13.3. Data subjects' right to correct their personal information



| Section 24 (Correction of personal information)

A data subject may ask an institution to correct inaccurate, out-of-date, incomplete, or misleading personal information in its possession or under its control. The POPIA Regulations prescribe a form that the data subject should use to request a correction to their personal information.¹²⁹

The institution must confirm the identity of the data subject before it implements the requested corrections.

If the institution decides not to comply with the request and if it is reasonable in the circumstances, the data subject may ask the institution to attach an indication to the information that the data subject requested a correction which was not made.

If the institution takes steps to change information that will impact past, present, or future decisions regarding the data subject, the institution must, if practicable, inform each person or organisation to whom the information has been disclosed of those steps.

The institution must inform the data subjects of any actions taken due to the request.

4.13.4. Data subjects' right to request the deletion or destruction of their personal information



| Section 24 (Correction of personal information)

A data subject may ask an institution to:

- delete excessive, irrelevant, out-of-date, incomplete, misleading, or unlawfully obtained personal information that it possesses or controls; and

¹²⁷ The fees are set out in Annexure B to the PAIA regulations available at: <https://infoeregulator.org.za/wp-content/uploads/2020/07/20210827-gg45057gon757-PAIAreulations-1.pdf>

¹²⁸ Regulation 8 of PAIA, available at: <https://infoeregulator.org.za/wp-content/uploads/2020/07/Form-3-PAIA.pdf>.

¹²⁹ Regulation 3(2), Form 2 available at: <https://infoeregulator.org.za/wp-content/uploads/2020/07/FORM-2-REQUEST-FOR-CORRECTION-OR-DELETION-OF-PERSONAL-INFORMATION-OR.pdf>

- destroy or delete personal information that the institution is no longer authorised to retain.¹³⁰

The data subject must use a form that the POPIA Regulations prescribe to request that the institution delete or destroy their personal information.¹³¹

The institution must confirm the identity of the data subject making the request before the institution can delete or destroy the personal information.

The institution must first consider if it has valid grounds to refuse the data subject's request to delete or destroy their personal information.

The institution has valid grounds to retain the personal information of the data subject if that information is necessary:

- to exercise the right to freedom of expression and information;
- to comply with a legal or contractual obligation;
- for lawful purposes related to the institution's functions or activities;
- for archiving purposes in the public interest;
- for scientific, statistical, or historical research purposes; or
- to establish, exercise, or defend legal rights and claims.

The institution must respond to the data subject's request as soon as possible by:

- destroying or deleting the personal information and confirming these actions to the data subject; or
- providing the data subject with evidence and reasons why the institution will not comply with their request.

4.13.5. Data subjects' right to object to the processing of their personal information



| Section 11(3)(a) (Consent, justification and objection)

Data subjects can object to the processing of their personal information on reasonable grounds related to their situation if the institution relies on any one of these legal bases¹³², namely that the:

¹³⁰ See section 4.11 for guidelines on record retention.

¹³¹ Regulation 3(2), Form 2 available at <https://infoeregulator.org.za/wp-content/uploads/2020/07/FORM-2-REQUEST-FOR-CORRECTION-OR-DELETION-OF-PERSONAL-INFORMATION-OR.pdf>

¹³² See section 4.5 for a discussion of the legal bases for processing personal information.

- processing is protecting a legitimate interest of a data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary to pursue the legitimate interests of the institution or of a third party to whom the information is supplied.

The POPIA Regulations prescribe a form that data subjects may use to object.¹³³ Once the data subject objected and if it was found that the objection was reasonable, the institution must stop processing the personal information, unless processing is justified by legislation.

4.13.6. Data subjects' right to opt out of and unsubscribe from direct marketing



Section 11(3)(b) (Consent, justification and objection)

Section 69(3) (Direct marketing by means of unsolicited electronic communication)

Data subjects have an absolute right to unsubscribe from or opt out of direct marketing. If the data subject provided consent for direct marketing in the past, they can withdraw that consent at any time. Every direct marketing communication must contain the details of the institution and an address, contact details or method for unsubscribing.

Institutions must provide ways for data subjects to withdraw their consent that are:

- free of charge; and
- free of unnecessary formality (i.e., it should be easy to unsubscribe).



Recommendation:

Institutions should follow these guidelines in providing ways for data subjects to unsubscribe:

- It must be simple for data subjects to opt out of or unsubscribe from direct marketing.
- When first collecting the data subject's details the consent and opt-out options must be presented as part of the same process (e.g., the consent and opt-out must be on the form the data subject completes).
- In subsequent communication, the data subject should be able to unsubscribe by replying to the message or by clicking on an unsubscribe link.

¹³³ Form 1 available at: <https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-1-OBJECTION-TO-THE-PROCESSING-OF-PERSONAL-INFORMATION.pdf>

- If the marketing is by SMS, the data subject should be able to reply STOP without incurring any costs.

4.13.7. Data subjects' right to not be subject to automated decisions based on profiles



| Section 71(3) (Automated decision-making)

Data subjects have the right to not be subject to automated decisions based on profiles, unless the institution can rely on one of the exceptions provided in section 72(2) discussed in paragraph 4.5.10.

If an institution makes automated decisions based on profiles in connection with the conclusion or execution of a contract and the request of the data subject has not been met, the institution must:

- provide an opportunity for a data subject to make representations about the decision; and
- provide a data subject with sufficient information about the underlying logic of the automated processing to enable them to make representations.

5. HOW TO ASSESS POPIA COMPLIANCE OF SPECIFIC PROCESSING ACTIVITIES

5.1. HOW TO ASSESS COMPLIANCE WHEN SHARING PERSONAL INFORMATION

This section highlights when institutions share personal information with third parties, how institutions must assess their processing activities when they share personal information with third parties and the contractual requirements for sharing personal information with third parties.

This section does **not** cover sharing personal information among employees of the institution and between the institution and an operator.¹³⁴



A **third party** is a person or institution that is not an operator or employee of the institution, for instance:

- other universities;
- funders;
- researchers not employed by the institution;
- the government; and

¹³⁴ Sharing personal information with operators is discussed in paragraph 4.10.

- parents of students.

5.1.1. When institutions share personal information with third parties

Institutions share personal information when they transfer that information to a third party or give a third party access to the information.

5.1.2. How to assess sharing

Every time an institution considers sharing personal information with a third party, the institution must assess that sharing activity to determine whether the activity complies with each of the conditions for the lawful processing of personal information; this means the institution must perform a PIIA.

To assess the sharing activity the institution must follow certain steps, namely:

- determine what personal information is shared;
- determine and document the purpose for sharing the personal information;
- identify who is accountable for POPIA compliance;
- assess whether the institution needs prior authorisation;
- determine whether personal information will travel across borders and assess the level of protection provided outside of South Africa;
- identify the legal basis for sharing;
- confirm that an exemption to the direct collection rule applies;
- assess whether the notification requirements have been met;
- assess whether sharing complies with the principle of minimal processing;
- assess whether the means of sharing is secure; and
- determine whether the institution can honour the rights of data subjects.

5.1.2.1. Determine what personal information is being shared

To assess the sharing activity, institutions must document exactly what personal information is being shared and in what format.



Example: Pension fund

An institution shares personal information of employees with a pension fund. The pension fund is the responsible party for managing the employee pension fund and needs monthly reports from the institution to fulfil their purposes. The institution submits monthly reports to a software solution used by the pension fund, the software provider is the pension fund's operator. Before the institution starts sharing employee information, it must determine

exactly what data fields are required by the pension fund and how the reports will be submitted.

5.1.2.2. Determine and document the purpose for sharing

To assess the sharing activity, institutions must document the purpose for which the personal information is being shared. It often happens that information was originally collected for a different purpose than the purpose for sharing. This may indicate that the sharing activity is further processing of the personal information and that an additional notification must be sent to the data subject.



Example: Donations from alumni

A student's personal information was collected when the student applied and was used during their studies at the institution. Several years after graduation, the institution wants to contact the alumnus to ask for a donation. This is an example of further processing, and the institution must determine whether the new purpose is compatible with the original purpose of collection. If not, the institution must ask for the consent of the alumnus.

5.1.2.3. Identify who is accountable for POPIA compliance

Institutions must determine who exactly the personal information is being shared with. When sharing personal information with other responsible parties, it is important that the parties involved determine who is accountable for POPIA compliance related to the activity. For instance, the institution that originally collected the information from the data subject must inform the data subject of the sharing activity. Similarly, the third party collecting the personal information from the institution may need to notify the data subject of their collection from the institution. Ideally, institutions should cover any overlapping or joint responsibilities in a written contract with the third party.

5.1.2.4. Assess whether the institution needs prior authorisation

Institutions may need to apply for authorisation from the data subject before they share personal information. For instance where an institution shares a child's personal information or a data subject's special personal information with a third party in another country.

5.1.2.5. Determine whether personal information will travel across borders and assess the level of protection provided outside South Africa



Section 72 (Transfers of personal information outside the Republic)

Institutions must consider the additional requirements when they intend to transfer personal information across borders. Institutions may only transfer personal information to third parties in foreign countries if:¹³⁵

¹³⁵ It is important to note that Section 72 only applies to the transfer to 'third parties'. This means that it does not apply to the use of foreign operators.

- the third party is subject to a law, binding corporate rules, or a binding agreement which provides an adequate level of protection. Protection will be 'adequate' if the law, rules, or agreement is 'effective', if it upholds principles for reasonable processing of personal information that are substantially similar to the principles in POPIA, and if it includes provisions about the further transfer to another third party in a foreign country that are substantially similar to section 72.
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the institution and the data subject, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary to conclude or perform in terms of a contract concluded in the interest of the data subject between the institution and the third party; or
- the transfer is for the benefit of the data subject, and if it is not reasonably practicable to obtain the consent of the data subject, and if it were reasonably practicable to obtain consent, the data subject would have been likely to give it.



Example: Exchange student programme

An institution has an exchange student programme with a university in New York. The applications to take part in the exchange programme are shared with the New York university to identify students that qualify for the programme. In this case, the institution can share the information across borders because the transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.

5.1.2.6. Identify the legal basis for sharing

All processing activities must have a legal basis for sharing as described in paragraph 4.5.

If the sharing activity was contemplated at the time that the personal information was collected, the institution must identify and document the legal basis that they relied on.

If the sharing activity was not contemplated at the time that the personal information was collected, the institution must consider whether the purpose for sharing is compatible with the original purpose of collection. How to assess whether further processing is authorised is described in paragraph 4.5.11.



Example: Qualification verification

A journalist contacts an institution to confirm that a politician obtained a particular qualification from that institution. The institution must consider whether it can rely on a legal basis in section 11 to share this information with the journalist. For instance, it may be in the politician's legitimate interest that their qualifications be confirmed. The institution must first obtain the data subject's consent before sharing this information.

Example: Sharing information with the government

Public universities must often share information with the government. In many instances, sharing personal information will be necessary to comply with legislation such as the Higher Education Act¹³⁶ or to properly perform a public law duty.¹³⁷

To assess whether sharing the personal information with the government is justified, the institution must gather the following information:

- What is the purpose for which the government is requesting access to the personal information?
- Can the institution justify sharing the personal information with the government for those purposes? In this case the sharing may be justified as long as it is necessary for the institution to comply with the Higher Education Act.
- Can the government justify using the personal information for those purposes? The government's justification will also be that it is complying with legislation.

If the purpose for which the government wants to use the information goes beyond complying with the Higher Education Act, that purpose must be justified on one of the other grounds in section 11, for instance, that the processing is necessary for the performance of a public law duty by a public body.

5.1.2.7. Confirm that an exemption to the direct collection rule applies

Before sharing personal information, it is wise for institutions to obtain confirmation from the third party that they may collect the information from the institution. In other words, an exception to the direct collection rule in section 12 must apply. This confirmation may be included in a contract with the third party as a warranty.

5.1.2.8. Assess whether the notification requirements have been met

Institutions must ensure that their privacy notices cover all sharing activities. As the institution's activities change, privacy notices must be updated and data subjects must be informed of any changes.

Section 18 requires that a data subject must be notified of the recipients or categories of recipients of the information and any intention of the institution to transfer the information to a foreign country, unless one of the exceptions in section 18(4) applies.¹³⁸

5.1.2.9. Assess whether sharing complies with the principle of minimal processing

In the context of information sharing activities, it is important for institutions to consider the following questions before they share personal information:

- Is it possible to achieve the same purpose without sharing the personal information?

¹³⁶ 101 of 1997.

¹³⁷ See paragraph 1.1.1.

¹³⁸ See paragraph 4.7.

- Is it possible to fulfil the same purpose with de-identified personal information?
- If personal information must be shared, is the minimum amount of personal information being shared?



Example: Graduation photos¹³⁹

A photography studio specialises in graduation photos and has made arrangements with an institution that it will give a discount to its students in exchange for access to the institution's database of graduates to market their services. The institution should ask itself a series of questions:

- **What is the purpose of sharing the personal information?** To make students aware of the discount.
- **Is there a way of achieving this purpose without having to share the students' personal information with the photography studio?** Yes, there is. The institution could make use of its usual communication channels for graduates to inform them of the discount.
- **If the institution does decide to share the graduates' information, is it sharing the minimum amount of information?** To fulfil this purpose, all the photography studio needs is a list of email addresses of graduates, nothing more.

5.1.2.10. Assess whether the means of sharing is secure



| Section 19 (Security measures on integrity and confidentiality of personal information)

Institutions must ensure that the means of sharing the personal information is secure and complies with the information security management requirements discussed in paragraph 4.9. The institution and the recipient of the information should agree in writing about taking adequate security measures before they share any personal information.



Example: Unauthorised sharing of personal information by WhatsApp

In April 2023 the Regulator issued an enforcement notice against the South African Police Services for breaching, amongst others, section 19. Sensitive personal information of data subjects was shared by a senior officer by WhatsApp. The information was subsequently forwarded to various SAPS WhatsApp groups. WhatsApp was not, at the time, an official authorised police messenger service and no policies or processes existed to implement appropriate security measures to manage access or distribution protocols. The information was shared widely outside the SAPS WhatsApp groups to other social media platforms.

¹³⁹ See De Stadler, Luttig Hattingh, Esselaar and Boast *Over-thinking the Protection of Personal Information Act* 392.

SAPS were ordered to publish an apology to the data subjects, investigate the officers involved and take appropriate internal disciplinary action against them, etc.¹⁴⁰

5.1.2.11. Determine whether the institution can honour the rights of data subjects

The institution must ensure that it can honour the rights of data subjects, such as the right to access personal information and to know who their personal information was shared with. An institution will only be able to honour these requests if they keep proper records of all sharing activities.

5.1.3. Contractual requirements when sharing with third parties

When institutions share personal information with third parties on a large scale or on a regular basis, it is best practice to conclude a personal information sharing agreement that contains a common set of rules that must be adopted by all parties involved.



Recommendation:

A personal information sharing agreement should document certain aspects of the sharing activity, namely:

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

¹⁴⁰ See <https://inforegulator.org.za/wp-content/uploads/2020/07/ENFORCEMENT-NOTICE-SAPS-MATTER-04052363.pdf>

- the obligations to maintain the quality of information;
- what appropriate indemnifications there are; and
- for how long the agreement will remain and what must happen with the personal information after the contract has come to an end.

5.2. HOW TO ASSESS COMPLIANCE OF DIRECT MARKETING



Section 1 (Definition of 'direct marketing' and 'electronic communication')

Section 69 (Direct marketing by means of unsolicited electronic communication)

In this section we cover when responsible parties market directly, when they need consent to market directly, when they can market directly without consent from data subjects, that data subjects have the right to opt out and unsubscribe from direct marketing and the best practice to follow with direct marketing.

5.2.1. When institutions market directly

Institutions generally market directly to prospective students, students, alumni and donors.



Direct marketing means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason.

The definition of direct marketing states that:

- the communication must be directed at an identified or identifiable data subject and not at the public in general; and
- the communication must have the purpose of promoting or offering goods or services for supply, or to request a donation.

POPIA covers all forms of direct marketing, including direct marketing in person, by mail, by fax, by telephone, with push notifications, by sending SMSs, emails, direct messaging on social media and through automatic calling machines.



Examples of direct marketing:

Institutions do direct marketing when they:

- promote their services at career days or open days in person;
- email individual scholars to invite them to apply;
- call alumni and request donations; and

- invite students to take part in campus activities.

Institutions do not do direct marketing when they:

- send out market research communications;
- send out notifications required by law; and
- communicate with students about their courses, examinations etc.

POPIA implements additional requirements for 'direct marketing by means of unsolicited electronic communication'.



Electronic communication means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Section 69 provides the following examples of electronic communications:

- calls made from automatic calling machines¹⁴¹
- facsimiles sent out by facsimile machines
- SMSs
- emails

Although direct marketing by telephone is not mentioned in section 69 or in the definition of electronic communication, the Regulator interprets the definition to include telephone calls.

5.2.2. When institutions need consent for direct marketing



| Section 69 (Direct marketing by means of unsolicited direct marketing)

Data subjects must give their consent before institutions can send them unsolicited direct marketing by means of electronic communication. This means that, when the institution communicates with the data subject for the first time, the institution must ask the data subject's permission to contact them again for direct marketing. This type of consent is sometimes referred to as opt-in consent. When institutions

¹⁴¹ Automatic calling machine is defined in section 69(5) as a machine that is able to do automated calls without human intervention.

intend to market directly to children – as prospective students of institutions are often under the age of 18 – the consent of their parent or guardian must first be obtained.

Section 69 states that an institution may only ask for a data subject's consent once. To ensure that institutions do not contact data subjects who withhold their consent, institutions must keep a record of data subjects who were asked for consent but who did not provide their consent.



Examples of unsolicited direct marketing by electronic communication are when institutions:

- collect email addresses of individuals that have 'director' in their title on LinkedIn and send emails to those individuals to ask for donations;
- send SMSs to individuals who partly completed an application form on their website, but who did not actually submit the application;
- obtain names and contact details from data brokers and send emails to those individuals marketing its postgraduate programmes; and
- send direct messages asking for donations to the members of an alumni Facebook group.

The POPIA Regulations prescribe that Form 4¹⁴² be followed by institutions and data subjects when obtaining the consent of data subjects for direct marketing.

Form 4 provides that the **institution** must complete the following fields:

- name of the data subject whose consent is requested
- name of the institution
- contact number of the institution
- fax number of the institution
- email address of the institution
- full names and designation of the person signing on behalf of the institution
- signature of the designated person
- the date of signature

Form 4 further provides that the **data subject** must complete these fields:

¹⁴² Available at: <https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-4-APPLICATION-FOR-THE-CONSENT-OF-A-DATA-SUBJECT-FOR-THE-PROCESSING-OF.pdf>

- full names of the data subject
- positive indication of giving consent (e.g., a box that must be ticked)
- a description of the goods or services that the institution may market
- the methods of communication with which the data subject wants to receive direct marketing (e.g., email, SMS, fax)
- the signature of the data subject
- the date and place of signature

Institutions do not have to use Form 4 exactly, but all the essential elements of the form must be present when they obtain consent.¹⁴³

5.2.3. When institutions can market directly without obtaining prior consent



| Section 69(3) (Direct marketing by means of unsolicited electronic communication)

Institutions may market directly in person and by post without obtaining the data subject's prior consent. POPIA also allows for a more lenient approach when electronic direct marketing is sent to existing 'customers'. Institutions may market directly to data subjects without obtaining prior consent if the institutions:

- obtained the data subject's contact details in the context of the sale of a product or a service;
- obtained the data subject's contact details for the purpose of directly marketing the institution's own or similar products or services; and
- gave the data subject a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to the direct marketing at the time of collection and on every subsequent direct marketing communication they had with the data subject.



Examples of when institutions may send electronic direct marketing without obtaining consent:

An institution emails prospective students whose applications were unsuccessful for specific programmes to offer them alternative programmes for which they qualify.

¹⁴³See the definition of 'form' in Regulation 1 which provides that the forms that are attached to the POPIA Regulations must be used 'or any form which is substantially similar to that form'.

An institution sends a fax to an organisation that offered student bursaries in the past, to request sponsorship of the fees of underprivileged students.

An institution emails graduates who recently earned undergraduate qualifications to promote relevant postgraduate programmes.

5.2.4. Data subjects' right to opt out and unsubscribe from direct marketing



Section 5 (Rights of data subjects)

Institutions must always allow data subjects to object (unsubscribe, opt out) to direct marketing, regardless of how they communicate. To do this, institutions must provide data subjects with means to unsubscribe or opt out every time institutions send data subjects a direct marketing communication, including the very first message. Once a data subject has unsubscribed to direct marketing, the institution must stop sending them direct marketing and keep a record of the unsubscribe to ensure that no further direct marketing is sent to the data subject in future.

The rights of data subjects to unsubscribe are discussed in paragraph 4.13.6.

5.3. HOW TO ASSESS COMPLIANCE OF AN INFORMATION MATCHING PROGRAMME

This section explains what an information matching programme is and sets out the additional measures that institutions must implement when they use information matching programmes that process personal information.



Section 40(1)(b)(ix)(bb) (Powers, duties and functions of the Regulator)

Section 44(2) (Regulator to have regard to certain matters)

5.3.1. What is an information matching programme

POPIA deals specifically with a processing activity referred to as 'information matching programmes'. This is defined as 'the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject'.¹⁴⁴

¹⁴⁴ The definition of 'information matching programme' in section 1.

5.3.2. Additional measures institutions must implement when using information matching programmes

POPIA does not contain specific rules relating to information matching programmes. However, because information matching programmes have the potential to invade the privacy of large numbers of data subjects, POPIA states that codes of conduct must 'specify appropriate measures for information matching programmes'¹⁴⁵ and places additional duties on the Regulator to monitor legislation that provides for personal information in information matching programmes in both the public and private sectors.¹⁴⁶ To determine whether the information matching programme complies with POPIA, the Regulator must consider the following issues:¹⁴⁷

- Does the objective of the programme relate to a matter of significant public importance?
- Does the use of the programme for this purpose result in significant and quantifiable monetary savings or other benefits?
- Are there alternative means of achieving the same purpose?
- Does the public interest in allowing the programme to proceed, outweigh the public interest in complying with the principles of POPIA?
- Does the programme involve information matching at an excessive scale regarding the number of private bodies involved and the amount of detail about a data subject that will be matched?



Example: Government database

The government wants to create a database of learners by combining the educational records of the Department of Basic Education with those of the Department of Higher Education to create a complete educational record of the lifetime of the learners.

If an institution wants to take part in an information matching programme the institution should consider whether the public or private body responsible for the programme has:

- conducted a privacy impact assessment of the programme;
- taken steps to comply with the principles of POPIA;
- taken steps to ensure that the public or private bodies who use the information matching programme is doing so in a POPIA compliant manner;

¹⁴⁵ Section 60(4)(a)(i).

¹⁴⁶ Section 40(1)(b)(ix)(bb).

¹⁴⁷ Section 44(2).

- made sure that the algorithms used to match the information has been validated and reviewed externally to ensure that they are valid, useful, fair and appropriate;
- put measures in place to regularly assess the quality of the personal information used in the information matching programme;
- provided all data subjects whose personal information is used in the matching programme with meaningful access to the personal information and created the opportunity for the data subjects to make representations about the accuracy of the information; and
- ensured that, if a negative result is generated (e.g., the matching programme reveals that a person does not have a qualification they claim to have), the information is not used in making significant decisions about the data subject before the data subject is informed of the negative result and given an opportunity to make representations.

Information matching programmes always make use of [unique identifiers](#) to link and combine personal information of a particular data subject from different sources. If an information matching programme also makes use of 'unique identifiers', the responsible party(s) may have to apply for prior authorisation from the Regulator. Prior authorisation is discussed in paragraph 4.5.12.

Information matching programmes are often used to produce or verify the personal information used in automated decision-making. Automated decision-making is discussed in paragraph 4.5.10.

6. POPIA COMPLIANCE PROGRAMMES

This section discusses the elements of a POPIA compliance framework, how to manage change brought about by POPIA compliance programmes, how to acquire executive sponsorship, consult with stakeholders and how to define roles and responsibilities within POPIA compliance programmes. To be able to become POPIA compliant, institutions must also develop certain policies. Three policies are then discussed as well as how to implement those policies. The section continues with a guideline on how to do a PIIA and how to monitor and continually improve compliance of institutions before it gives tips for how institutions should prepare for an assessment of the Regulator.

6.1. THE ELEMENTS OF A POPIA COMPLIANCE FRAMEWORK

One of the responsibilities of an Information Officer is to ensure that a compliance framework is developed, implemented, monitored, and maintained.¹⁴⁸ This POPIA framework consists of all the interrelated and interacting components within an institution. A POPIA compliance framework:

¹⁴⁸ Item 4(1)(a) of the POPIA Regulations.

- sets out the institution's approach to manage POPIA risks by addressing aspects, such as compliance strategy, objectives, governance, policy, roles and responsibilities, compliance risk appetite, process, techniques, and reporting;
- establishes and maintains (or contributes to, supports, facilitates, enables establishing and maintaining) POPIA compliance-related objectives and the activities, policies, procedures, processes and practices to achieve those objectives; and
- directs, guides, contributes to, facilitates, enables or supports related practices and activities related to POPIA compliance.¹⁴⁹

For institutions that already have a compliance framework, managing POPIA compliance risks would form part of that larger framework.

To start a POPIA compliance programme the institution must obtain executive sponsorship and buy-in. The institution must further identify and consult stakeholders to determine the roles, responsibilities and policies that must be developed and implemented. Thereafter, the institution must monitor and audit compliance and improve compliance if and where necessary.

The rest of this section describes the steps that the Information Officer, supported by their Deputy Information Officers, should follow to implement a POPIA compliance programme.

¹⁴⁹ This definition is adapted from the Generally Accepted Compliance Framework issued by the Compliance Institute South Africa.

Figure 6: POPIA compliance framework



6.2. HOW TO MANAGE CHANGE

Change management is built around a set of practices that are based on understanding how people respond to change. In other words, change management helps to effectively prepare, equip, and support people through change. As with project management, change management requires a plan, however where a project management plan would focus on costs and deliverables, a change management plan focuses on the changes that are required in the mindsets, skills and knowledge of people to achieve POPIA compliance. The protection of personal information is, after all, a people problem. The success of a POPIA compliance programme depends on how well the institution manages change; and the worst outcome of a POPIA compliance programme would be that nothing changes.

For institutions, change management is crucial in becoming POPIA compliant because:

- an institution must change the way it operates – if people do not adopt these changes, POPIA compliance will remain elusive;
- human error is one of the leading causes of data breaches, which means that training people should be a large component of any POPIA compliance programme; and
- some employees will have new roles requiring new skills (e.g., Information Officers, Deputy Information Officers, privacy champions etc.).



Recommendation:

Information Officers must create a change management plan. A change management plan focuses on the changes that the institution must make to become POPIA compliant. These changes can include changes in mindsets, skills, and knowledge. Information Officers should answer these questions in their change management plan:

- Why should the institution comply with POPIA? The key is to understand that different groups of people within the institution are motivated by different things.
- What needs to change to achieve POPIA compliance?
- Who needs to be involved in the POPIA compliance programme? I.e., who are the stakeholders?
- How and when do things need to change? A communication and training plan is essential to achieving POPIA compliance.

Useful resources:

- The UK's information regulator – the ICO – has [a guide and tool](#) to help organisations create their own 'accountability framework' for privacy risk management. Although the guide and tool were created for GDPR purposes, it can easily be adapted for purposes of POPIA as the core principles are the same. Also look at the ICO's page on [training and awareness](#) as it has valuable information.
- The IAPP has a wealth of [resources](#) on data privacy training and awareness.
- The Centre for Information Policy Leadership published an excellent report in 2020 called '[What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework](#)'. This report provides guidance on all the essential elements for a POPIA compliance framework and contains case studies from many international organisations including several universities about what has and has not worked for their data privacy compliance programmes.
- For a good example of a regular compliance framework by an Australian university go to [Deakin University Australia's compliance management framework](#) which can easily be adapted to incorporate the elements of a POPIA compliance framework.

6.3. HOW TO GET EXECUTIVE SPONSORSHIP

POPIA affects most processes in an institution, so having the support of leadership is vital in establishing a sustainable, and well-funded POPIA compliance programme.

A POPIA compliance programme needs buy-in and budget from leadership. Here are some arguments to convince executives that POPIA compliance is worth investing in:

- Data breaches can be very costly. According to IBM the global average cost of a data breach in 2023 was USD 4.45 million. This includes the cost of regulatory fines, civil liability,

disruptions in operations, business continuity risk, unexpected expenses, and the loss of goodwill.¹⁵⁰

- A POPIA compliance programme can save an institution money. POPIA programmes can mitigate losses from data breaches, enable agility and innovation, achieve operational efficiency from data controls, make the institution more attractive to investors and build loyalty and trust with stakeholders.
- By embedding privacy in the structures of the institution, the institution can attract stakeholders who feel very strongly about privacy (so-called privacy actives).

Other institutions are investing in privacy. It is pivotal that South African public universities keep up with international standards to stay competitive.

Useful resources:

For the ‘carrot approach’

- CISCO and the Centre for Information Policy Leadership published a report in 2023 called [‘Business Benefits of Investing in Data Privacy Management Programs’](#). This study shows that organisations can gain considerable financial advantages by investing in accountability frameworks, including the use of a privacy maturity model.
- CISCO’s [‘Privacy as an Enabler of Customer Trust’](#) 2024 benchmark study shows that privacy is an extremely important factor when a customer chooses an institution.
- McKinsey discusses how companies can gain a competitive edge through robust data protection strategies, especially as consumers become increasingly cautious about sharing their data, in their article [‘The consumer-data opportunity and the privacy imperative’](#).

For the ‘stick approach’

IBM’s annual [‘Cost of a data breach report 2023’](#) outlines exactly how expensive data breaches are – and how taking preventative measures can save organisations large amounts of money if a data breach occurs.

A university example

[South African Universities](#) are being targeted for ransomware and cybersecurity attacks.

6.4. HOW TO CONSULT WITH STAKEHOLDERS

To become POPIA compliant, and by extension, to implement a POPIA programme is an immense exercise in teamwork and coordination, so stakeholder consultation is essential. If an institution fails to manage important stakeholders it can undermine a POPIA compliance programme.

¹⁵⁰ IBM’s Cost of a Data Breach report 2023 is available at <https://www.ibm.com/reports/data-breach>.

Information Officers should identify the following stakeholders:

- Those who govern the change: Who are the decision-makers? Who approves new policies? Who are the leaders?
- Those who must give input: Who will help develop new policies and procedures? Who understands the impacts of new policies and procedures?
- Those who are affected by the change: Who will need to change how they work?
- Those who support your need: Who in the institution already has some of the skills required to implement a POPIA compliance programme?

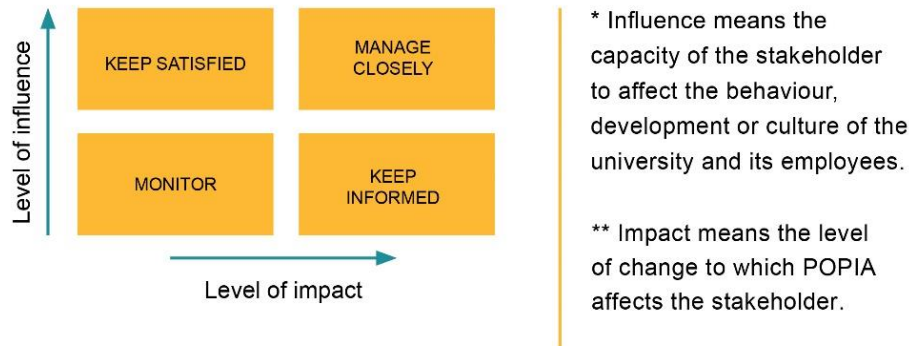
One way to identify stakeholders is to make a chart of the different functional areas within an institution, for instance:

Figure 7: Functional areas within an institution



Once stakeholders have been identified, Information Officers should assess the impact of the POPIA compliance programme on each stakeholder. Information Officers can determine how they should engage a stakeholder by assessing the level of influence of the stakeholder and the degree to which the POPIA programme will affect them.

Figure 8: Assessing the impact of the POPIA compliance programme on each stakeholder



A stakeholder engagement plan should include the following information for each stakeholder:

- What kind of impact would POPIA compliance have on the stakeholder's activities?
- Does the stakeholder already fulfil some of the functions required for POPIA compliance?
- Can the stakeholder assist with POPIA compliance initiatives?
- How can the POPIA programme assist the stakeholder?

Useful resources:

- The IAPP's series of articles on stakeholder engagement for privacy programmes called [‘the three As of successful privacy programmes’](#).
- The global head of privacy at Keywords Studios, Dominga Leone's LinkedIn article on [‘How to get buy-in for your privacy programme’](#).
- An article of Forbes giving seven tips on [‘How To Work With Operations And Marketing Teams For A Successful Privacy Program’](#).

6.5. HOW TO DEFINE ROLES AND RESPONSIBILITIES

In risk and compliance management, it is considered best practice to follow the three lines of defence model. This model is based on the idea that all three lines of defence must work together and function optimally to provide structure around properly complying with POPIA and managing POPIA compliance risk. The roles and responsibilities are illustrated in the following diagram.

Figure 9: The role of the three lines of defence in POPIA compliance



Ensure that the responsibilities created by the institution's POPIA compliance programme are included in the institution's performance management systems so that individuals know what is expected of them to continuously improve their performance.

The institution must follow these steps as part of their performance management:

- Align individual and team goals with the strategic objectives of the institution's POPIA compliance programme. Document these goals, e.g., in key performance indicators.
- Develop plans to achieve these goals.
- Review and assess the progress of individuals and teams.

Incorporate training to develop individuals' POPIA knowledge, skills and abilities.

Useful resources:

- The Institute of Internal Auditors' paper that explains the '[three lines of defence model](#)'.
- The CIPL's 2020 report about '[What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework](#)'. This report gives an excellent overview of how to pick your 'privacy team', how reporting lines for managing privacy-related risks can work, and how to integrate privacy within risk management.
- Durham University's (UK) example of [how to set out your roles and responsibilities in data privacy compliance](#). Although this was done with reference to the GDPR, it can easily be applied to POPIA.

6.6. WHICH POLICIES TO DEVELOP

POPIA does not require that institutions must have policies in place to ensure the protection of personal information. If institutions implemented 'compliance controls' they would, as a rule, meet the compliance obligations that POPIA imposes. These controls are 'generally incorporated in an organisation's policies, procedures, processes, people, practice and structures, systems and technology.'¹⁵¹

To achieve full POPIA compliance, institutions should have the following policies:

- A privacy policy
- An information security management policy
- A records management policy

¹⁵¹See the definition of 'compliance control' in the GACP.

These policies are distinct from one another because they apply to different classes of information. While a privacy policy would only apply to personal information, an information security management policy and a records management policy would apply to all types of information.

6.6.1. Privacy policy

A privacy policy ensures that the institution proactively complies with all relevant privacy regulations and that the institution respects data subjects' right to privacy.

Topics it should address	Corresponding sections in POPIA
Information classification	Sections 5, 14, 17, 18, 19, 22, 23, 26-35
Documenting personal information processing activities	Sections 17, 18, 22, 23, 24
Purpose specification	Sections 10, 13, 14, 15, 17, 18, 69 read with Form 4 of the POPIA 2018 Regulations
Legal basis for processing activities	Sections 11, 26-35, 69 read with Item 6 and Form 4 of the POPIA 2018 Regulations
Minimality	Sections 10 and 14
Lawful sources	Sections 12, 16, 18
Transparency	Sections 5, 13, 14, 15, 17, 18, 23
Information quality	Sections 5, 10, 12, 14, 16, 23(2), 24, 71, Item 3 read with Form 2
Limit sharing with third parties	Sections 10, 11, 13, 19, 20, 21, 22, 23(2), 72
Personal information impact assessments	Item 4(b) of the POPIA 2018 Regulations
Records retention periods	Section 14
Data subjects' rights	Sections 5, 18, 22, 23, 24, 25, 69 read with Form 4, of the POPIA 2018 Regulations, Item 2 read with Form 1, Item 3 read with Form 2, Item 4(c) and (d), Item 7 read with Part I of Form 5 and Part II of Form 5 of the POPIA 2018 Regulations

Responsible, empowered users	Item 4(e) of the POPIA 2018 Regulations
Information security (a cross reference to the ISM Policy)	Sections 14, 19, 20, 21, 22
Incident management and response (may be same process as ISM policy)	Sections 19, 21, 22

Institutions should also develop a data subject request procedure which sets out how to respond to requests of data subjects to access and correct, to delete, and to object to the processing of their personal information.

Useful resources:

- For your data privacy policy (remember this is not your privacy notice on your website!), the IAPP has [template examples](#) that you can adapt for POPIA purposes.
- The ICO's accountability framework has a specific section [on data subject access requests](#).
- Look at the IAPP's [data subject access request template](#).
- The Universities of [Edinburgh](#) and [Manchester](#) both have good examples of a data subject access request portals and procedures.

6.6.2. Information security management policy

Information security management policies apply to all types of information, not just personal information. A typical policy about information management describes how the institution secures information against:

- breaches of confidentiality;
- failures of integrity; and
- interruptions to the availability of information.

Topics it should address	Corresponding sections in POPIA
Information classification	Sections 5, 14, 17, 18, 19, 22, 23, 26-35
Access control	Sections 11, 26-35, 69 read with Item 6 and Form 4 of the POPIA 2018 Regulations
Third-party management	Sections 10, 11, 13, 19, 20, 21, 22, 23(2), 72

Information quality	Sections 5, 10, 12, 14, 16, 23(2), 24, 71, Item 3 read with Form 2
Availability and business continuity	Section 19, 20, 22
Compliance with binding rules (e.g., all relevant privacy regulations, corporate governance standards, internal policies and contractual obligations)	
Responsible, empowered users	Item 4(e) of the POPIA 2018 Regulations
Clear roles and responsibilities in the implementation of the policy	Section 19, 20, 21
Information security assessments	Section 19

Useful resources:

- For an information security management policy, the best source is the ISO 27001 standard.
- Heimdal Security is a cybersecurity provider who has shared why it is extremely important to have an information security policy and provided a [template](#) to use. Heimdal Security is also a provider of cloud-based security solutions.

6.6.3. Records management policy

A records management policy applies to all types of information, not just personal information.

A records management policy ensures that the institution's recordkeeping:

- is transparent, consistent, and accurate;
- meets legal, regulatory, fiscal, operational, and historical requirements;
- supports the efficient conduct of its business; and
- ensures the preservation of archives documenting its history and development.

Topics it should address	Corresponding sections in POPIA
Comply with all legal and operational recordkeeping requirements and create a records retention schedule	Section 14(1)(a),(b)
Secure destruction	Section 14(4),(5)

Information security (a cross reference to the ISM policy)	Sections 14, 19, 20, 21, 22
Effective version control	Section 14(6),(7),(8), sections 5, 10, 12, 14, 16, 23(2), 24, 71, Item 3 read with Form 2
Minimise duplication by identifying and controlling master records	Section 10, 14
Manage and preserve knowledge and intellectual property	
Incident management and response (may be the same process as ISM policy)	Sections 19, 21, 22
Responsible, empowered users	Item 4(e) of the POPIA 2018 Regulations
Clear roles and responsibilities in the implementation of the policy	Sections 19, 20, 21
Records management assessments	Item 4(b) of the POPIA 2018. Regulations

Useful resources:

- The ICO of the UK, has a page on what is expected to be included in a [records management policy](#) and gives examples of how companies can meet these requirements.
- The UK-based JISC has a good [guide for records management at universities](#).

6.7. HOW TO IMPLEMENT POLICIES

Policies must be followed, owned, updated and used to test compliance against. An institution's policy is successful when the compliance of that institution can be measured against the policy through an internal or external audit and when the policy is routinely used to address non-compliance.

To develop a policy implementation plan, institutions should ask the following:

Figure 10: Questions institutions should ask to develop a policy implementation plan



- The **implementation team** mostly consists of the policy owner (usually the Information Officer or Deputy Information Officers) and representatives of senior management. This team will involve other people when particular skill sets are required.
- Policies rarely exist in isolation. They are often referenced in **other policies and supporting documents**. When an institution adopts a new policy, the policy implementation team should assess whether other policies must be amended. Policies will have to be amended if they govern specific personal information processing activities or if there is an opportunity to insert POPIA controls in processes governed by other policies.
- A new privacy policy will have an **impact on any business process** that involves personal information. Institutions can assess the impact of the policy on these processes by doing PIAs to identify instances where the process does not comply with the policy and to manage risk that is caused by that non-compliance. The implementation plan must also determine how the institution will assess changes to processes due to the introduction of new processes to ensure that these changes do not introduce new POPIA compliance risks.
- New policies may require new **infrastructure and equipment**.

It is vital to assess the impact of a new policy on **people**. Institutions must ask who will have to do their job differently because of a new policy, whether they have the knowledge and skill to make these changes, and if not, what kind of training they will require.



Example:

One of the policy statements of an institution's Records Management Policy is that personal information must be destroyed securely. How will the institution do this? The institution will need special software for digital information and shredders for paper records.

If an institution's Information Security Management Policy provides that access to personal information must be restricted to employees who 'need to know', is it still appropriate for the institution to have open plan offices?

Useful resources:

- The Centre for Information Policy Leadership published a report in 2020 that gives a good overview and tips on how to implement privacy-related policies and procedures within an organisation; ['What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework'](#).
- The UK's information regulator – the ICO – released a guide and tool to assist organisations to create their own '[accountability framework](#)' for [privacy risk management](#). Although the guide and tool were created for GDPR purposes, they can easily be adapted for POPIA purposes as the core principles remain the same. There is a specific resource dedicated to implementing privacy-related policies and procedures within an organisation.
- Berkeley University has [a change-management toolkit](#) which can assist institutions with implementing their new policies and procedures.

6.8. HOW TO DO PERSONAL INFORMATION IMPACT ASSESSMENTS

Performing PIAs helps institutions assess, analyse and evaluate POPIA compliance risk. If the institution has not done any POPIA compliance assessments before, all processing activities should be assessed to identify risks and a plan should be developed to address those risks.

To do a PIA, institutions can follow an eight-step approach. Institutions must:

- identify when to do the PIA;
- do an inherent risk assessment;
- describe the processing activity;
- identify privacy risks;
- identify and evaluate risk-mitigation measures;
- document the outcomes;
- integrate those outcomes into a project plan; and
- agree on a monitoring plan.

6.8.1. Identify when to do a PIA

If a process, project, initiative, contract or activity involves personal information, an institution should do a PIA. Employees in key positions should be trained to recognise personal information so they can trigger a PIA. For instance, asking whether personal information is involved should be a standard part of an institution's project management lifecycle and procurement process.

6.8.2. Do an inherent risk assessment

The inherent risk-rating would determine the institution's next steps. If an activity is inherently low in risk, the institution may choose to accept the risk and continue with the activity 'as is'. If the activity is inherently high in risk, the institution should assess the risk further to determine what risk-mitigation steps it should take.

To assist institutions in doing inherent risk assessments, they should create a questionnaire designed to identify processes or activities that have inherently high privacy risks. This questionnaire could, for example, consider:

- the volume of personal information processed;
- whether any special personal information or personal information of children is involved;
- whether the processing is 'further processing';
- whether the processing involves profiling and automated decision-making;

- whether the processing is invisible (i.e., if the data subject is unaware of the processing or would be surprised by it);
- whether the institution needs prior authorisation to do the processing;
- the value of the personal information (e.g., what would it cost to replace the personal information if it was lost);
- how disruptive it would be if the processing activity was interrupted or if the personal information was no longer available (i.e., how important is this particular processing activity to the organisation); and
- how valuable personal information would be to a bad actor.

6.8.3. Describe the processing activity

Institutions must document all the steps in the processing activity to fully understand how personal information is being processed. Institutions could use data flow mapping to track the data life cycle and document how personal information is collected, used, transferred, shared, archived and destroyed.

6.8.4. Identify privacy risks

Institutions can use questionnaires and interviews to identify privacy risks. The activity must be assessed against the policy statements in the institution's Privacy Policy, Information Security Management Policy and Records Management Policy.

The purpose of this process is to provide a list of all possible POPIA risks, regardless of whether there are existing controls that address them. It is appropriate to include both risks to the data subject and the institution.

6.8.5. Identify and evaluate risk mitigation measures

The aim is to identify solutions that eliminate the risk or reduce the risk to a level that is acceptable to the institution.

Institutions should record solutions in a risk response plan, such as that the institution could:

- accept the risk without further action as some risks may be unlikely or low-impact;
- put a contract in place that provides assurance or transfers the liability;
- develop a privacy notice to improve transparency;
- introduce a new policy or amend an existing one;
- introduce a procedure to manage the risk;
- disable certain features of a product or service;
- train people to be aware of the risk and how to avoid it;

- implement technical measures like enforcing strong encryption or preventing certain actions; or
- abandon the processing activity.

These solutions may not eliminate POPIA-compliance risk completely which is why institutions should identify and rate the residual risks to ensure that they are comfortable with the level of residual risk that the processing activity poses.

6.8.6. Document outcomes

Depending on how the institution has defined its roles and responsibilities and provided that senior management is the first line of defence,¹⁵² senior management must decide how to treat POPIA risks and which solutions to implement. It is senior management's responsibility to follow the procedure and to respond to the POPIA risks that are identified.

The Information Officer is the second line of defence, which means that their primary role is to advise, monitor and report. In other words, it is the Information Officer's role to ensure that there is a PIIA procedure in place.

6.8.7. Integrate the outcomes into a project plan

Institutions should integrate the risk response plan into a project plan to ensure that there is a clear plan and an implementation timeline and that actions are assigned to a responsible person.

6.8.8. Agree on a monitoring plan

The Information Officer, the relevant member of senior management, and internal audit should agree on a monitoring plan to ensure that the agreed solutions have been implemented, that the risk does not recur and that new risks are managed in future.

Resources:

- The ICO has [a good guideline](#) for PIIAs.
- UK-based UCISA's [Privacy Impact Assessment toolkit](#) is excellent. Remember, in terms of POPIA, institutions must always do PIIAs, whereas the GDPR only requires them in certain cases.
- [Edinburgh University](#) has a very thorough resource page on privacy impact assessments.

[Bristol University](#) has a useful screening questionnaire template to determine if you need to conduct a PIIA with a full PIIA assessment template.

¹⁵² Refer to the three lines of defence in paragraph 6.5.

6.9. HOW TO MONITOR AND CONTINUALLY IMPROVE COMPLIANCE

The institution's Information Officers must ensure that the performance and effectiveness of its POPIA compliance framework is evaluated and its shortcomings addressed. To do this the institute must determine the following:

- What must be monitored and measured?
- Which methods will be used for monitoring and measurement?
- When will monitoring and measurement happen?
- Who will do the monitoring and measurement?
- When will the results be analysed and evaluated?
- Who will analyse and evaluate the results?

The Information Officers must ensure that this process and any outcomes are documented.

Resources:

- The Centre for Information Policy Leadership published a thorough report in 2020 called '[What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework](#)'. This report gives a good overview and tips on how to monitor and sustain compliance with your privacy framework, policies and procedures.
- The ICO has a guide and tool to help organisations create their own '[accountability framework](#)' for privacy risk management. The guide and tool were created for GDPR purposes, but are easy to adapt for POPIA purposes as the core principles remain the same.
- The IAPP has a series of articles about [monitoring compliance with privacy programmes](#).

6.10. HOW TO PREPARE FOR AN ASSESSMENT FROM THE REGULATOR



| Section 76 (Action on receipt of a complaint)

The Regulator may investigate or assess institutions' compliance with POPIA at any time on their own initiative, or to investigate complaints received from any person. In case of an assessment or investigation, an institution must provide evidence of compliance, such as:

- registration certificates of the institution's Information Officer and Deputy Information Officers;

- the institution's POPIA compliance framework including its internal Privacy Policy, data subject request procedure, Information Security Management Policy, security compromise or data breach procedure, Records Management Policy and records retention schedule;
- proof that it performed PIAs and that it had completed a POPIA-compliance risk register and project plan to address risks identified;
- proof that the institution provided training about and awareness of POPIA compliance to all its employees;
- privacy notices;
- signed contracts with all the institution's operators; and
- proof that the institution identified and assessed information security risks and that appropriate safeguards have been implemented (e.g., generally accepted information security practices and procedures that have been implemented).

7. GLOSSARY

Automated means	Any equipment capable of operating automatically in response to instructions given for the purpose of processing information.
Binding Corporate Rules	Binding Corporate Rules are Personal Information Processing policies within a group of undertakings that must be adhered to by a Responsible Party or Operator within that group of undertakings when transferring Personal Information to a Responsible Party or Operator within that same group of undertakings in a foreign country. A group of undertakings means a controlling undertaking and its controlled undertakings.
Child	A natural person under 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning themselves.
Competent Person	Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	The person to whom personal information relates.

De-identify	In relation to personal information of a data subject, de-identify means to delete any information that: (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and "de-identified" has a corresponding meaning.
Direct Marketing	To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason.
Electronic Communication	Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or the recipient's terminal equipment until it is collected by the recipient.
Filing system	Any structured set of personal information, whether centralised, decentralised, or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
Information Matching Programme	The comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about 10 or more data subjects, with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used to take any action in regard to an identifiable data subject.
Information Officer	Of, or in relation to, a: (a) public body, means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or (b) private body, means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.
Legitimate Interest Assessment	A balancing test of the responsible party or third party's interest against the data subject's rights and interests.
Operator	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
Person	A natural person or a juristic person.
Personal Information	Information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited

	to: (a) 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; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) 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; (g) the views or opinions of another individual about the person; and (h) 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.
Personal Information Impact Assessment/PIIA	An assessment which is used to assess whether a process complies with POPIA.
Processing	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information
PAIA	The Promotion of Access to Information Act 2 of 2000 and its Regulations
POPIA	The Protection of Personal Information Act 4 of 2013 and its Regulations
Profiling	Means any form of automated processing of personal information to evaluate certain aspects relating to a data subject.
Public Body	Means: (a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when: (1) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

	(2) exercising a public power or performing a public function in terms of any legislation.
Public Record	A record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Record	Any recorded information: (a) regardless of form or medium, including any of the following: (i) writing on any material; (ii) information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Regulator	The Information Regulator established in terms of section 39 of POPIA. ¹⁵³
Responsible Party	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
Special Personal Information	Personal information concerning: (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to: (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Third Party	Means a natural or legal person, public body, agency, or body other than the data subject, responsible party, operator, and persons who, under the direct authority of the responsible party or operator, are authorised to process personal information.

¹⁵³ More information about the Regulator is available on their website <https://info regulator.org.za/>.

Unique Identifier	Any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.
-------------------	---